Уманський державний педагогічний університет імені Павла Тичини
Факультет фізики, математики та інформатики
Кафедра інформатики і інформаційно-комунікаційних технологій

«**ЗАТВЕРДЖУЮ**»
Завідувач кафедри
_____ Марія МЕДВЕДЄВА
«8» серпня 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК 25. ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ

Галузь знань 01 Освіта / Педагогіка

Спеціальність 014.09 Середня освіта (Інформатика)

Освітня програма Середня освіта (Інформатика)

Умань – 2022

Робоча програма з дисципліни «Основи Інтернету Речей» для здобувачів вищої освіти спеціальності 014.09 Середня освіта (Інформатика).

Розробники: старший викладач кафедри інформатики і інформаційно-комунікаційних технологій Паршуков С.В.

Робочу програму схвалено на засіданні кафедри інформатики і інформаційно-комунікаційних технологій
Протокол № 1 від «08» серпня 2022 року

Завідувач кафедри інформатики і інформаційно-комунікаційних технологій
_____ Медведєва М.О.

Робочу програму розглянуто та затверджено на засіданні науково-методичної комісії факультету фізики, математики та інформатики

Протокол № 1 від «08» серпня 2022 року
Голова науково-методичної комісії факультету фізики, математики та інформатики
_____доц. Тягай І.М.

Пролонговано:
на 20__/20__ н. р. _____ (_____) «__» ___ 20__ р., протокол № __
(підпис) (ПІБ)
на 20__/20__ н. р. _____ (_____) «__» ___ 20__ р., протокол № __
(підпис) (ПІБ)
на 20__/20__ н. р. _____ (_____) «__» ___ 20__ р., протокол № __
(підпис) (ПІБ)
на 20__/20__ н. р. _____ (_____) «__» ___ 20__ р., протокол № __
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни (обов'язкова чи вибіркова)	обов'язкова	обов'язкова
Мова викладання, навчання та оцінювання	українська	українська
Загальний обсяг у кредитах ЄКТС / годинах	5 / 150	5 / 150
Курс	I	I
Семестр	2	1,2
Кількість змістових модулів із розподілом:	4	4
Обсяг кредитів	5	5
Обсяг годин, у тому числі:	150	150
Аудиторні:		
Лекційні	34	6
Семінарські / Практичні		
Лабораторні	40	10
Самостійна робота	76	134
Індивідуальні завдання	-	-
Форма семестрового контролю	екзамен	екзамен

2. Мета й завдання навчальної дисципліни

Мета: оволодіння базовими теоретичними знаннями та практичними навичками з проектування та побудови системи IoT для вирішення конкретних завдань.

Після проходження курсу студенти зможуть виконувати такі задачі: налаштовувати пристрій IoT для підключення до мережі; використовувати Python для створення програм, які приймають вхідні дані від користувача і зчитують та записують до зовнішніх файлів; пояснювати поняття Великі Дані; працювати в середовищі програмного пакету Cisco Packet Tracer; здійснювати захист пристроїв IoT; розрізняти середовища передачі даних; виконувати тестування мережних підключень.

3. Результати навчання за дисципліною

Вивчення дисципліни має на меті сформувати наступні загальні і професійні компетентності та отримати такі програмні результати навчання як:

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі середньої освіти, педагогіки та інформаційних технологій, що передбачає застосування концептуальних методів освітніх наук, теорії та методики навчання інформатики і характеризуються комплексністю та невизначеністю умов організації освітнього процесу в закладах загальної середньої освіти (базова середня освіта).

ЗК 2. Здатність до міжособистісної взаємодії, роботи в команді, спілкування з представниками інших професійних груп різного рівня (соціальна компетентність).

ПК 3. Інформаційно-цифрова компетентність як здатність: орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, оперувати нею у професійні і й діяльності; ефективно використовувати наявні та створювати (за потреби) нові електронні (цифрові) освітні ресурси; використовувати цифрові технології в освітньому процесі;

ПК 13. Інноваційна компетентність як здатність: застосовувати наукові методи пізнання в освітньому процесі; використовувати інновації у професійній діяльності; застосовувані різноманітні підходи до розв'язання проблем у педагогічній діяльності;

ПК 14. Здатність до навчання впродовж життя як здатність: визначати умови та ресурси професійного розвитку впродовж життя; взаємодіяти з іншими вчителями на засадах партнерства та підтримки (у рамках наставництва, супервізії тощо).

Програмні результати навчання:

ПРН 1. Знає основні історичні етапи розвитку предметної галузі.

ПРН 4. Знає та розуміє структуру предметної галузі, місце інформатики в системі наук, розуміє перспективи розвитку інформаційно-комунікаційних технологій та їхнє суспільне значення.

ПРН 5. Знає та розуміє фізичні, логічні та математичні основи інформатики та інформаційно-комунікаційних технологій.

ПРН 7. Знає дидактичний потенціал та технічні можливості апаратно-програмних засобів для ефективної організації освітнього процесу.

ПРН 8. Оперує базовими категоріями та поняттями предметної галузі, в тому числі загальноприйнятою міжнародною ІТ-термінологією.

ПРН 9. Застосовує знання нормативно-правових документів та міжнародних й національних стандартів для ефективної організації професійної та громадської діяльності.

ПРН 12. Уміє реалізувати алгоритми розв'язання задач мовами програмування, вибирати й застосовувати інформаційно-комунікаційні технології для розв'язування задач шкільного курсу інформатики різного рівня складності.

ПРН 13. Уміє використовувати апаратне та програмне забезпечення, враховує принципи функціонування пристроїв та вимоги до їх експлуатації при організації освітнього процесу.

ПРН 14. Володіє прийомами, методами та засобами ефективного пошуку інформації, критичного аналізу та опрацювання даних для використання у професійній діяльності з дотримання принципів академічної доброчесності.

ПРН 15. Вміє використовувати та добирати засоби ІКТ для розв'язання конкретних задач у професійній діяльності (проєктування інформаційно-освітнього середовища та його окремих компонент, створення програмних засобів, розробки вебресурсів тощо).

ПРН 20. Здатний самостійно приймати рішення на основі сформованих ціннісних орієнтирів та моральної автономії, що дозволяє, зберігаючи людську гідність і доброчесність, бути вільним від зовнішнього тиску, диктату влади, усталених норм, думки інших; управляти складною технічною або професійною діяльністю; спроможний нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих або навчальних контекстах.

4. Програма навчальної дисципліни

Змістовий модуль 1. Вступ до Інтернету Речей

Тема 1. Все підключено.

Знайомство з курсом. Програмне та інформаційне забезпечення. Огляд навігації по матеріалам курсу. Цифровізація трансформує все. Глобально пов'язані через мережі. Зростання кількості IoT пристроїв. Підключення пристроїв до мережі.

Тема 2. Всі речі можна програмувати.

Основні підходи програмування. Основи програмування з використанням Програмування з використанням Python. Що таке прототипування. Ресурси для прототипування.

Тема 3. Все навколо створює дані.

Що таке Великі Дані. Де зберігаються Великі Дані. Аналіз та візуалізація даних.

Тема 4. Все може бути автоматизованим.

Автоматизація та її використання. Штучний інтелект і машинне навчання. Мережі на основі намірів.

Тема 5. Все має бути захищеним.

Важливість безпеки даних. Захист корпоративних даних. Захист персональних даних та пристроїв.

Тема 6. Освітні та ділові можливості.

Виклики та можливості в цифровому світі. Освітні та професійні можливості. Навчальна програма академії. Галузеві сертифікати.

Змістовий модуль 2. З'єднання речей

Тема 7. Речі та зв'язки.

Інтернет речей. Складові блоки системи IoT. Процеси в керованих системах. Моделі спілкування. Рівні з'єднань. Вплив зв'язків на конфіденційність та безпеку.

Тема 8. Датчики, виконавчі механізми та мікроконтролери.

Основні терміни та поняття електроніки. Розширена термінологія та концепції електроніки. Від схематичного зображення до макета та друкованої плати. Введення в пакет інструментів SparkFun Inventor's Kit, мікроконтролер Arduino. Прості схеми з Arduino IDE. Зондування довкілля за допомогою датчиків. Виконавчі механізми та реле. Модель End-toEnd IoT-системи.

Тема 9. Програмне забезпечення є скрізь.

Що таке код? Код виконує роботу! IoT пристрої та обробка даних. Апаратне забезпечення Raspberry Pi. Доступ до програми Raspberry Pi віддалено за допомогою PL-додатка. Використання операційної системи Linux. Blockly. Python на Raspberry Pi. Використання Raspberry Pi. Модель системи IoT.

Тема 10. Мережі, туманні та хмарні обчислення.

Роль мережі. Бездротові технології. Туманні та хмарні сервіси. Великі дані. Безпека в IoT.

Тема 11. Застосування IoT.

Огляд системи IoT від Cisco. Захист даних, площин управління та речей в системах Cisco IoT. Індустрії та ринки IoT. Підключення охорони здоров'я. Розумні міста. Розумні мережі. Підключене виробництво.

Тема 12. Створи IoT рішення.

Вирішення глобальних проблем. Технології, що трансформуються в усьому світі. Проектування рішень. Проект системи IoT. Прототип системи IoT. Бізнес модель Canvas. Навички 21 століття.

Змістовий модуль 3. Безпека Інтернету Речей

Тема 13. IoT під атакою.

Незахищені підключені речі. Ризик унікальної партії. NICE та IoT системи. Використання IoT в розумному будинку. Використання IoT в охороні здоров'я. Лабораторне середовище дослідження безпеки IoT.

Тема 14. Системи та архітектури IoT.

Мережні моделі. IoT моделі. Рівні безпеки IoT. Вимоги до безпеки IoT. Аналіз моделі загроз.

Тема 15. Атаки на пристрої IoT.

Апаратні компоненти IoT. Програмні компоненти IoT. Безпека обладнання. Вразливості прошивки. Концепції керування доступом до мережі. Шифрування.

Тема 16. Атаки на рівень зв'язку.

Функції рівня зв'язку IoT. Бездротові протоколи. Вразливості протоколу IP. Вразливості TCP та UDP протоколу. Безпека рівня зв'язку.

Тема 17. Атаки на додатки IoT.

Вразливості локальних додатків. Вразливості Web та хмарних додатків. Рівень додатків IoT. Усунення проблем із безпекою в протоколах обміну повідомленнями.

Тема 18. Оцінка вразливостей та ризиків у системі IoT.

Оцінка вразливості. Типи та інструменти перевірки вразливості. Концепції та підходи до оцінки ризиків. Оцінка ризику з визначенням загрози. Ідентифікація загроз та пріоритезація ризиків. Управління ризиками в системах IoT. Загальні відомості про Blockchain. Як працює Blockchain.

Змістовий модуль 4. Хакатон для студентів

Тема 19. Дизайнерське мислення.

Концепції дизайну та Інтернету речей. Психологічні концепції для кращого дизайну. Методи школи дизайну Стендфорда.

Тема 20. Підготовка до хакатону.

Ща таке хакатон? Деталі хакатону. Очікування та результати від хакатону.

5. 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
Модуль 1												
Змістовий модуль 1. Вступ до Інтернету Речей												
Тема 1. Все підключено	6	2		2		2	6	2				4
Тема 2. Всі речі можна програмувати	6	2		2		2	6			2		4
Тема 3. Все навколо створює дані	8	2		2		4	8					8
Тема 4. Все може бути автоматизованим	8	2		2		4	8			2		6
Тема 5. Все має бути захищеним	8	2		2		4	8					8
Тема 6. Освітні та ділові можливості	2					2	2					2
Разом за змістовим модулем 1	38	10		10		18	38	2		4		32
Змістовий модуль 2. З'єднання речей												
Тема 7. Речі та зв'язки	6	2		2		2	6	2				4
Тема 8. Датчики, виконавчі механізми та мікроконтролери	8	2		2		4	8			2		6
Тема 9. Програмне забезпечення є скрізь	10	2		4		4	10			4		6
Тема 10. Мережі, туманні та хмарні обчислення	8	2		2		4	8					8

Тема 11. Застосування IoT	10	2		2		6	10					10
Тема 12. Створи IoT рішення	4					4	4					4
Разом за змістовим модулем 2	46	10		12		24	46	2		6		38
Змістовий модуль 3. Безпека Інтернету Речей												
Тема 13. IoT під атакою	6	2				4	6	2				4
Тема 14. Системи та архітектури IoT	6	2		2		2	6					6
Тема 15. Атаки на пристрої IoT	8	2		4		2	8					8
Тема 16. Атаки на рівень зв'язку	8	2		6		2	8					8
Тема 17. Атаки на додатки IoT	8	2		4		2	8					8
Тема 18. Оцінка вразливостей та ризиків у системі IoT	6	2		2		2	6					6
Разом за змістовим модулем 3	44	12		18		14	44	2				42
Змістовий модуль 4. Хакатон для студентів												
Тема 19. Дизайнерське мислення	10	1				9	10					10
Тема 20. Підготовка студентів до хакатону	12	1				11	12					12
Разом за змістовим модулем 4	22	2				20	22					22
Усього годин	150	34		40		76	150	6		10		134
Модуль 2												
ІНДЗ			-	-		-			-	-		-
Усього годин	150	34		40		76	150	6		10		134

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1.	Налаштування Pl-App із Raspberry Pi	2	2
2.	Використання Pl-App Notebook	2	2
3.	Мигання світлодіодом з використанням Raspberry Pi і Pl-App	2	2
4.	Основні команди Linux	2	2
5.	Блимаючий світлодіод за допомогою Redboard та Arduino IDE	2	2
6.	Фоторезистор за допомогою Redboard та Arduino IDE	2	
7.	Цифровий осцилограф	2	
8.	Датчик згину та сервомотор	2	
9.	Реле	2	
10.	Світлодіодна лінія та графіки за допомогою PL-App	2	
11.	Керування світлодіодами за допомогою PL-App Dashboard	2	
12.	Захист Raspberry Pi	2	

13.	Створення системи датчика-приводу IoT	2	
14.	Компромісне обладнання пристрою IoT	2	
15.	Прослуховування Bluetooth за допомогою Raspberry Pi	2	
16.	Сканування портів пристрою IoT	2	
17.	Створення пакетів для використання незахищених портів	2	
18.	Вразливість веб-додатків	2	
19.	Злом MQTT	2	
20.	Вразливості UPnP	2	

8. Самостійна робота

Короткий опис форми самостійної роботи і змісту навчального матеріалу для студентів.

№ з/п	Зміст навчального матеріалу	Кількість годин	
		Денна форма	Заочна форма
1.	Наскільки Ви підключені	0,5	0,5
2.	Створення карти Інтернету	0,5	0,5
3.	Уявлення нового інтелектуального сенсору	0,5	0,5
4.	Переваги та недоліки пристроїв IoT	0,5	0,5
5.	Створення Блок-схем	0,5	0,5
6.	Основи програмування мовою Python	1	1
7.	Створення простої гри із використанням Python IDLE	1	1
8.	Налаштування віртуалізованого серверного середовища	1	1
9.	Введення до Arduino	1	1
10.	Дослідження великого набору даних	1	1
11.	Використання Excel для прогнозування	1	1
12.	Автоматизація повсякденних подій	1	1
13.	Розробка прототипу ШІ додатку	1	1
14.	Дослідження мережі на основі намірів (IBN)	1	1
15.	Види даних	0,5	0,5
16.	Інтернет-відбиток пальців	0,5	0,5
17.	Дослідження ризиків своєї поведінки в Інтернеті	0,5	0,5
18.	Професії, пов’язані з IoT та навчальні можливості	0,5	0,5
19.	Аналіз процесу	1	1
20.	Система управління з відкритим зв’язком	1	1
21.	Порівняння системи керування із замкнутим та розімкнутим зв’язком	1	1
22.	Діаграма процесу	1	1
23.	Діаграма процесу реального світу	1	1
24.	Світ працює на схемах	1	1
25.	Проектування схеми від початку до кінця	1	1
26.	Написання скриптів Python за допомогою блоків	1	1
27.	Написання простих скриптів мовою Python	1	1
28.	Написання скриптів мовою Python з використанням текстового редактора	1	1
29.	Проектування схеми від початку до кінця	1	1
30.	Packet Tracer. Розгортання та з’єднання пристроїв	1	1
31.	Packet Tracer. Створення простої мережі з використанням Packet Tracer	1	1
32.	Packet Tracer. Додавання IoT пристроїв до розумного будинку	1	1
33.	Packet Tracer. Підключення та моніторинг пристроїв IoT	1	1

34.	Packet Tracer. Мигання світлодіодом з використанням Blockly	1	1
35.	Packet Tracer. Дослідження розумного будинку	1	1
36.	Packet Tracer. Налаштування бездротової безпеки	1	1
37.	Дослідження світу професіоналів зкібербезпеки	0,5	0,5
38.	Робота з Webex Teams	1	1
39.	Взаємодія з фізичним світом через Webex Teams	1	1
40.	Взаємодія коду Arduino та Python	1	1
41.	Packet Tracer. Підключення пристроїв для побудови IoT	1	1
42.	Packet Tracer. Моделювання пристроїв IoT	1	1
43.	Packet Tracer. Датчики та мікроконтролер PT	1	1
44.	Packet Tracer. SBC актуалізація з Python	1	1
45.	Packet Tracer. Дослідження розумного будинку	1	1
46.	Вертикальні та горизонтальні ринки	1	1
47.	Система аварійної зупинки електростанції під час землетрусу	1	1
48.	Робота з IFTTT та Google акаунтами	1	1
49.	Блок схема свого проекту	1	1
50.	Електрична схема свого проекту	1	1
51.	Діаграма послідовності свого проекту	1	1
52.	Схід і захід сонця в Google календарі за допомогою IFTTT	1	1
53.	Діаграма бізнес-моделей	1	1
54.	Packet Tracer. Створення рішення заводського підключення	1	1
55.	Packet Tracer. Забезпечення хмарних сервісів в IoT	1	1
56.	Packet Tracer. Розумне місто	1	1
57.	Packet Tracer. Розумний Grid	1	1
58.	Packet Tracer. Прототип та перевірка рішення	1	1
59.	Packet Tracer. Моделювання загроз на рівні пристрою	1	1
60.	Packet Tracer. Моделювання загроз на комунікаційному рівні IoT	1	1
61.	Packet Tracer. Моделювання загроз на рівні пристрою IoT	1	1
62.	Packet Tracer. Моделювання загроз для оцінки ризику в системі IoT	1	1
63.	Пошук Шодана	1	1
64.	Оцінка останніх атак IoT	1	1
65.	Оцінка продуктів домашньої автоматизації	1	1
66.	Оцінка ризиків безпеки IoT у галузевому секторі	1	1
67.	Налаштування топології лабораторії безпеки IoT	1	1
68.	Дослідження інструментів оцінки вразливостей	1	1
69.	Дослідження вимог безпеки IoT	1	1
70.	Дослідження бази даних FCC	1	1
71.	Компромісне прошивка пристрою IoT	1	1
72.	Використання OpenVAS для оцінки вразливостей	1	1
73.	Перевірка паролів за допомогою інструментів Kali	1	1
74.	Використання CVSS	1	1
75.	Оцінка ризиків за допомогою DREAD	1	1
76.	Blockchain Demo 2.0	1	1
77.	Прискорений курс від Stanford d.school	1	1
78.	Свіжий погляд	1	1
79.	Зачаровані об’єкти	1	1
80.	Cisco Prototyping Lab	2	2
81.	Фоторезистор за допомогою Redboard та Arduino IDE		2

82.	Цифровий осцилограф		2
83.	Датчик згину та сервомотор		2
84.	Реле		2
85.	Світлодіодна лінія та графіки за допомогою PL-App		2
86.	Керування світлодіодами за допомогою PL-App Dashboard		2
87.	Захист Raspberry Pi		2
88.	Створення системи датчика-приводу IoT		2
89.	Компромісне обладнання пристрою IoT		2
90.	Прослуховування Bluetooth за допомогою Raspberry Pi		2
91.	Сканування портів пристрою IoT		2
92.	Створення пакетів для використання незахищених портів		2
93.	Вразливість веб-додатків		2
94.	Злом MQTT		2
95.	Вразливості UPnP		2
96.	Опрацювання теоретичного матеріалу		28

9. Індивідуальні завдання

Індивідуальні завдання не передбачені.

10. Методи навчання

Лекції (онлайн, офлайн, змішані) із використанням презентаційних матеріалів; виконання лабораторних робіт в емуляторі Cisco Packet Tracer та на реальному обладнанні; самостійна онлайн робота з курсами «Вступ до Інтернету Речей», «Основи Інтернету Речей: з'єднання речей», «Основи Інтернету Речей: безпека IoT» та «Основи Інтернету Речей: підготовка до Хакатону» на платформі Netacad та «Exploring IoT with Cisco Packet Tracer», «Introduction to Internet of Things» та «Introduction to Cybersecurity» на платформі Skills For All, яка передбачає розгляд матеріалів електронних підручників, відпрацювання термінів та понять, проходження тестування з тем, завантаження звітів лабораторних робіт в систему на перевірку.

11. Методи контролю

Самоконтроль перевірки розуміння теоретичного матеріалу та розуміння термінів і понять; перевірка результатів (звітів) лабораторних робіт; проходження тестування.

12. Критерії оцінювання результатів навчання

Контрольні роботи з тем, тест з курсів (модулів) оцінюються за 100 бальною шкалою (перевірка здійснюється автоматично системою). Студент має від 3 до 10 спроб в залежності від виду тесту. Звіти про виконання лабораторних робіт оцінюються викладачем з відміткою виконано або не виконано (потрібно доробити / переробити з додаванням коментаря). Всі види тестів потрібно скласти мінімум на 60 балів, в журнал оцінок заноситься остання спроба, яка і буде враховуватися при підрахунку загальної кількості балів за дисципліну. Дисципліна вважається пройденою, якщо виконані і оцінені лабораторні роботи, пройдені всі тести та заповнено відгук про курс. Якщо студента не задовольняє отримана оцінка і він використав всі доступні спроби, він складає екзамен.

13. Розподіл балів, які отримують здобувачі вищої освіти

Самоконтроль																		ЗМ1 тест	ЗМ2 тест	ЗМ3 тест	ЗМ4 тест	Екзамен
Змістовий модуль 1						Змістовий модуль 2						Змістовий модуль 3										
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	Т17	Т18					
100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	10

T1, T2 ... T12 – теми змістових модулів.

Загальна оцінка за дисципліну підраховується за формулою: 0,2*ЗМ1 тест+0,3*ЗМ2 тест +0,3*ЗМ3 тест +0,1*ЗМ4 тест +Екзамен

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка в ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсової роботи, практики	для заліку
90–100	A	відмінно	зараховано
82–89	B	добре	
75–81	C		
69–74	D	задовільно	
60–68	E		
35–59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1–34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

14. Рекомендована література

Основна

1. Грінгард С. Інтернет речей / пер. О. Герасимчук. Харків : Книжк. клуб «Клуб Сімейн. Дозвілля», 2018. 176 с.
2. Інтернет речей для індустріальних і гуманітарних застосунків / ред. В. Харченко. Харків : Нац. аерокосм. ун-т ХАІ, 2019. Т. 1 : Основи і технології. 547 с.
3. Роуз Д. Дивовижні технології. Дизайн та інтернет речей / пер. з англ Д. Гломозда. Харків : Книжк. клуб «Клуб Сімейн. Дозвілля», 2018. 335 с.

Допоміжна

1. Monk S. Movement, light, and sound with arduino and raspberry pi. San Francisco : Maker Media, 2016. 336 p.
2. Monk S. Practical electronic recipes with arduino and raspberry pi. Boston : O'Reilly Media, 2017. 480 p.

15. Інформаційні ресурси

1. Exploring IoT with Cisco Packet Tracer - Skills for All. URL: https://skillsforall.com/course/exploring-iot-cisco-packet-tracer?userLang=en-US (date of access: 08.08.2022).
2. Introduction to Cybersecurity - Skills for All. URL: https://skillsforall.com/course/introduction-to-cybersecurity?userLang=en-US (date of access: 08.08.2022).
3. Introduction to Internet of Things (IoT) - Skills for All. URL: https://skillsforall.com/course/introduction-iot?userLang=en-US (date of access: 08.08.2022).
4. Introduction to IoT. Networking Academy. URL: https://www.netacad.com/courses/iot/introduction-iot (date of access: 08.08.2022).
5. IoT Fundamentals: connecting things. Networking Academy. URL: https://www.netacad.com/courses/iot/iot-fundamentals (date of access: 08.08.2022).
6. IoT Fundamentals: Hackathon Playbook. *Networking Academy*. URL: https://www.netacad.com/courses/iot/hackathon-playbook (date of access: 08.08.2022).
7. IoT Fundamentals: IoT Security. *Networking Academy*. URL: https://www.netacad.com/courses/cybersecurity/iot-security (date of access: 08.08.2022).