Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ЦТЕ

Кафедра цифрових технологій в енергетиці

Основи технології Інтернету речей (IoT)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Цифрові технології в енергетиці*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*3 курс, осінній семестр*
Обсяг дисципліни	*4/120 год 36 лек 18 лаб 66СРС*
Семестровий контроль/ контрольні заходи	*Залік/МКР*
Розклад занять	*http://roz.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com, тел.063-863-97-30 Лабораторні роботи: к.т.н, доц. Довженко Надія Михайлівна, nadezhdadovzhenko@gmail.com, тел.063-863-97-30*
Розміщення курсу	*https://campus.kpi.ua*

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Навчальна дисципліна **«Основи технології Інтернету речей (IoT)»** покликана сформувати у студентів компетентності, необхідні для проєктування архітектури та компонентів IoT мереж, систем «Розумний будинок» та «Розумне місто»; при розробці, впровадженні та управлінні IoT-рішеннями, інтегруванні різноманітних пристроїв у єдину екосистему, а також для моніторингу та забезпечення безпеки даних і систем.

Програмою дисципліни **«Основи технології Інтернету речей (IoT)»** передбачається вивчення особливостей побудови й експлуатації складових компонентів IoT мереж, зокрема їх характеристик, протоколів та технологій передачі інформації та загальних підходів до моделювання сегментів мереж таких систем, як «Розумний будинок» та «Розумне місто».

Метою навчальної дисципліни є формування у студентів здатностей:

- до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем (ФК 3);
- застосовувати теоретичні та практичні основи методології та технології моделювання для дослідження характеристик і поведінки складних об'єктів і систем, проводити обчислювальні експерименти з обробкою й аналізом результатів (ФК 7);
- розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж (ФК 13);
- застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури (ФК 14).

Основні завдання навчальної дисципліни.

Згідно з вимогами освітньо-професійної програми студенти після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання:

- проєктувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислювальних функцій (ПР 5);
- використовувати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення (ПР 14);
- розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних (ПР 16).

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни необхідні знання та уміння за такими дисциплінами як «Алгоритмізація та програмування. Частина 1. Базові концепції програмування», «Алгоритмізація та програмування. Частина 2. Процедурне програмування», «Операційні системи», «Об'єктно-орієнтоване програмування».

Після вивчення дисципліни студенти зможуть використати набуті знання та вміння при вивченні: «Методи та системи штучного інтелекту», «Моделювання систем в енергетиці», та дипломному проєктуванні.

3. Зміст навчальної дисципліни

Тема 1. Вступ до IoT;
Тема 2-3. Архітектура IoT-мереж;
Тема 4. Розробка мереж IoT;
Тема 5-6. Підключення смарт-об'єктів;
Тема 7. IP як мережевий рівень IoT;
Тема 8. Протоколи рівня застосунків IoT;
Тема 9. Дані та аналітика для IoT;
Тема 10-11. Захист IoT;
Тема 12-13. Промисловий IoT;
Тема 14. Вступ до енергетичної галузі IoT;
Тема 15-16. «Розумний» будинок та «Розумні» міста;
Тема 17. Громадська безпека;
Тема 18. Комбінування рішень Blockchain, ШІ та IoT.

4. Навчальні матеріали та ресурси

Базова література:

1. Олещенко Л.М. Програмування пристроїв Інтернету речей / Л.М. Олещенко, Я.В. Хіцко. – К.: КПІ ім. Ігоря Сікорського, 2019, – 47 с.
2. Великий О.А. Мікроконтролери та мікропроцесорна техніка: методичні вказівки до практичних занять для здобувачів освітньо-професійної програми «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної форми навчання / уклад. О.А. Великий – Луцьк: ТК Луцького НТУ, 2019. – 80 с.
3. Новацький А.О. Мікропроцесорні та мікроконтролерні системи. Частина 1. Мікропроцесорні системи. Підручник. - Київ: КПІ ім. Ігоря Сікорського, Політехніка, 2020. – 361 с.
4. Новацький А.О. Мікропроцесорні та мікроконтролерні системи. Частина2. Проектування мікропроцесорних систем. Підручник. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 462 с.
5. Рябенький В.М., Ушкаренко О.О. Програмовані електронні системи керування, збору та обробки інформації. - Миколаїв: Іліон, 2021. – 490 с.
6. Dac-Nhuong Le, Chintan Bhatt, Mani Madhukar. Security Designs for the Cloud, IoT, and Social Networking. CRC Press, 2020.

7. Security and Privacy in Internet of Things (IoTs). Models, Algorithms, and Implementations. Fei Hu. CRC Press, 2016.

Додаткова література

1. Sathish Janani. Learn Arduino Products: All Arduino Boards, Tech Specs, Comparison, Software, Hardware, Code Functions. Amazon.com Services LLC, 2021
2. Introduction to IoT (Cisco Networking Academy) [Електронний ресурс]. – Режим доступу: https://www.netacad.com
3. Arduino Documentation [Електронний ресурс]. – Режим доступу: https://www.arduino.cc/en/Tutorial/HomePage
4. Arduino Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/arduino/index.htm

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

Тема 1. Вступ до IoT	
1	Еволюційні етапи розвитку мережі Інтернет. Четверта промислова революція (від Індустрії 1.0 до Індустрії 4.0). Переваги IoT для розумних підключених будівель. Цифрова стеля. Переваги PoE. Конвергенція IT і OT. Закони України, що регламентують роботу IoT. Міжнародні стандарти, що регламентують роботу IoT.
Тема 2-3. Архітектура IoT-мереж	
2	Архітектура корпоративної IT-мережі та IoT-мережі. Унікальні проблеми та архітектурні моделі IoT. драйвери IoT. Стандартизована архітектура oneM2M IoT. Стандартизована архітектура Всесвітнього форуму IoT (IoTWF).
3	Відповідальність IT та OT у еталонній моделі IoT. Модель Пердью для ієрархії управління. Еталонна архітектура для промислового Інтернету речей. IoT-A. IoT Data Management and Compute Stack. Core IoT Functional Stack. Управління даними IoT і стек обчислень
Тема 4. Розробка мереж IoT	
4	Типи датчиків. Мікроелектромеханічні системи (MEMS). Розумні об’єкти. Сенсорні мережі. Безпроводові сенсорні мережі (WSN)
Тема 5-6. Підключення смарт-об'єктів	
5	Підключення смарт-об'єктів. технології підключення розумних об’єктів. Мережі з обмеженими вузлами. Швидкість передачі даних і пропускна здатність. Технології доступу IoT. IEEE 802.15.4. Протокольні стеки.
6	Високорівневий протокольний стек ZigBee. Архітектура LoRaWAN. Безпека LoRaWAN. Неліцензовані LPWA технології. NB-IoT та інші варіації LTE. Варіанти розгортання NB-IoT. WirelessHART. Thread.
Тема 7. IP як мережевий рівень IoT	
7	Переваги набору протоколів IP для Інтернету речей. Бізнес-кейс для IP. Системи SCADA. Порівняння стека протоколів IoT, що використовує 6LoWPAN, та стека протоколів IP. Фрагментація. Mesh-Under проти Mesh-Over маршрутизації. Робоча група 6Lo. 6TiSCH
Тема 8. Протоколи рівня застосунків IoT	
8	Вимоги до багатоадресної передачі.. Протокол передачі телеметрії через чергу повідомлень (MQTT). Формат повідомлення MQTT. Обмежений протокол застосунків (CoAP). Стек протоколів IoT для CoAP і MQTT. Комунікації CoAP в інфраструктурах IoT.
Тема 9. Дані та аналітика для IoT	
9	Виклики традиційних систем управління даними. Огляд аналітики даних IoT. Типи аналізу даних. Еволюція машинного навчання та нейронні мережі. Застосування машинного навчання для IoT. Системи масового паралельного оброблення даних. NoSQL Бази даних. Екосистема Hadoop. Apache Kafka, Apache Storm та Apache Flink. Lambda Architecture
Тема 10-11. Захист IoT	
10	Вразливості та загрози в мережах IoT. Пріоритети безпеки. Modbus, DNP3. Протокол ICCP.
11	Безпека промислових мереж. Кроки та фази OCTAVE Allegro. Factor Analysis of Information Risk. Використання IDS/IPS

Тема 12-13. Промисловий IoT	
12	Стратегія IoT для підключеного виробництва. Архітектура Converged Plantwide Ethernet (CPwE).
13	Референсна модель систем автоматизації та керування промисловими процесами. Логічний фреймворк IACS. Протокол Resilient Ethernet Protocol (REP). Протоколи управління промисловою автоматизацією. Архітектура PROFINET
Тема 14. Вступ до енергетичної галузі IoT	
14	Традиційні етапи генерації, передачі та розподілу в мережі енергетичної компанії. Модель GridBlocks. Еталонна архітектура GridBlocks. Традиційна мережа SCADA. IEC 61850. Забезпечення безпеки «розумної» енергомережі. Стандарт безпеки NERC CIP.
Тема 15-16. «Розумний» будинок та «розумні» міста	
15	Архітектура «розумного» будинку. Загрози «розумного» будинку.
16	Стратегія IoT для «розумних» міст. Архітектура безпеки. Архітектура IoT для «розумних» міст. Приклади використання IoT у «розумних» містах.
Тема 17. Громадська безпека	
17	Проєкт IoT для громадської безпеки. Архітектура IoT для екстреного реагування (Мобільний командний центр). Мережеві служби та служби безпеки. MANET. IoT-рішення для наземних, повітряних та морських мобільних транспортних засобів. Обробка інформації IoT у сфері громадської безпеки
	Тема 18. Комбінування рішень Blockchain, ШІ та IoT
18	Роль Blockchain у забезпеченні безпеки та прозорості в IoT. Децентралізація даних. Штучний інтелект у керуванні IoT пристроями. Використання алгоритмів ШІ для аналізу даних з IoT пристроїв. Створення розумних контрактів (Smart Contracts) для автоматизації транзакцій в IoT мережах. Використання ШІ для оптимізації процесів в Blockchain системах. Приклади інтеграції Blockchain, ШІ та IoT у різних галузях (промисловість, охорона здоров'я, логістика тощо)

Лабораторні заняття

№ з/п	Назва	Кількість ауд. годин
1	Моделювання функціонування пристроїв IoT	4
2	Програмування пристроїв SBC із використанням Python	4
3	Дослідження особливостей функціонування «Розумного» будинку в середовищі Cisco Packet Tracer	6
4	Захист хмарних сервісів в IoT	4
	Всього	**18**

6. Самостійна робота студента

№ з/п	Назва теми, що виноситься на самостійне опрацювання	Кількість годин СРС
1	Створення простої мережі з використанням Cisco Packet Tracer	6
2	Типи пристроїв IoT, які підключаються до мережі	4
3	Основи програмування в Blockly	4
4	Штучний інтелект (ШІ) та його роль в IoT	4
5	Програмування в Python (Python IDLE)	6
6	Машинне навчання (МН) в IoT	4
7	Використання шифрування для забезпечення безпеки IoT	6
8	Приклади використання RFID технології в IoT	4
9	Архітектура розподілених обчислень для IoT	4
10	Моделювання мереж IoT з використанням симуляційних інструментів	6
11	Програмні платформи для розробки IoT рішень	4
12	Використання IoT у промислових додатках (Industrial IoT)	10
13	Принципи побудови інтелектуальних міст (Smart Cities) на базі IoT	4
	Всього	**66**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Для успішного проходження курсу та складання контрольних заходів необхідним є вивчення навчального матеріалу за кожною темою. Специфіка курсу передбачає набуття студентом необхідного рівня професійних знань у сфері проєктування архітектури та компонентів IoT мереж, розробки, впровадження й управління IoT-рішеннями, інтегрування різноманітних пристроїв у єдину екосистему, а також моніторингу та забезпечення безпеки даних і систем. Кожен студент повинен ознайомитися і слідувати Положенню про академічну доброчесність, Статуту і розпорядку дня університету.

- Відвідування лекцій та лабораторних занять, а також відсутність на них, не оцінюється.
- Під час захисту лабораторних робіт студент має продемонструвати розроблені IoT сегменти, програмні коди та результати їх виконання, які необхідні для управління елементами проєктованих мереж. У випадку дистанційної форми навчання захист відбувається на відповідній конференції шляхом демонстрації екрана.
- Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.
- Норми етичної поведінки Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

1) Рейтинг студента з кредитного модуля складається з балів, що він отримує за:
- виконання та захисту 4 лабораторних робіт;
- виконання 1 модульної контрольної роботи;

Максимальна кількість балів за всі завдання, виконані в семестрі, дорівнює:

15 х 4 (лабораторні роботи) +40балів (МКР) = 100 балів.

2) Критерії нарахування балів

2.1. Оцінюються 4 лабораторні роботи, передбачені програмою. Максимальна кількість балів – 15*4 = 60 балів. Рейтингові бали кожної роботи складаються з балів за правильність виконання (від 0 до 10) та захист роботи (від 0 до 3), балів за оформлення протоколу роботи (від 0 до 2).

2.2. Максимальна кількість балів за модульну контрольну роботу дорівнює 40 балів. На модульну контрольну роботу виноситься два питання. За кожну вірну відповідь на запитання надається 20 балів.

Умови допуску до заліку: мінімальна кількість набраних балів – 60 (60%).

3)Результати виконання залікової контрольної роботи оцінюється за 100-бальною шкалою.

Білет залікової контрольної роботи складається з двох теоретичних питань та одного практичного завдання. Ваговий бал кожного теоретичного питання – 30 балів, завдання – 40 балів.

Максимальна кількість балів за складання заліку дорівнює

30 балів *2 + 40 балів = 100 балів.

Теоретична частина оцінюється таким чином:

- правильна чітко викладена, повна відповідь – (не менше 90% потрібної інформації) – 27-30 балів;
- достатньо повна відповідь (не менше 75% потрібної інформації) – 23-26 балів;
- неповна відповідь (не менше 60% потрібної інформації) – 18-22 бали;
- незадовільна відповідь – 0 балів.

Практичне завдання оцінюється таким чином:

- повне, безпомилкове розв’язування завдання – 36-40 балів;
- повне, розв’язування завдання із несуттєвими невідповідностями – 30-35 балів;

- завдання виконане з певними недоліками – 24-29 балів;
- завдання не виконано – 0 балів.

4) Рейтингова оцінка за семестр за бажанням студента визначається одним з таких способів:
- кількість балів, отриманих за стартовою шкалою, або
- результат виконання залікової контрольної роботи (тоді не враховуються бали, отримані в семестрі, за умови, що їх кількість не менше 60).

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Бали	Оцінка
95 - 100	Відмінно
85 - 94	Дуже добре
75 - 84	Добре
65 - 74	Задовільно
60 - 64	Достатньо
Менше 60	Незадовільно
R < 40: незараховані лабораторні роботи або не виконані інші умови допуску	Не допущено

9.Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль:

1. Вплив цифрової трансформації на бізнес;
2. Інтелектуальний «розумний» пристрій та інтелектуальний сенсор;
3. Створення простої мережі з використанням Cisco Packet Tracer;
4. Типи пристроїв IoT, які підключаються до мережі;
5. Переваги та недоліки пристроїв IoT;
6. Основи програмування в Blockly;
7. Програмування в Python (Python IDLE);
8. Особливості використання у системах IoT «великих» даних;.
9. Аналіз великих наборів даних з пристроїв IoT;
10. Штучний інтелект (ШІ) та його роль в IoT;
11. Машинне навчання (МН) в IoT;
12. Комбінування рішень Blockchain, ШІ та IoT;
13. Алгоритми машинного навчання для аналізу даних IoT;
14. Особливості захисту середовища IoT;
15. Фізична безпека IoT пристроїв;
16. Захист персональних даних в IoT;
17. Використання шифрування для забезпечення безпеки IoT;
18. Види та засоби захисту від загроз в мережах IoT;
19. Протоколи передачі даних у мережах IoT;
20. Технології зв'язку для IoT (Wi-Fi, Bluetooth, Zigbee);
21. Енергоефективність пристроїв IoT;
22. Приклади використання RFID технології в IoT;
23. Роль хмарних обчислень у системах IoT;
24. Взаємодія IoT пристроїв з хмарними сервісами;
25. Архітектура розподілених обчислень для IoT;
26. Використання сенсорних мереж у системах IoT;
27. Архітектура сенсорних мереж;
28. Підключення сенсорів до IoT мереж;
29. Моделювання мереж IoT з використанням симуляційних інструментів;
30. Програмні платформи для розробки IoT рішень;
31. Використання IoT у промислових додатках (Industrial IoT);
32. Принципи побудови інтелектуальних міст (Smart Cities) на базі IoT;
33. Застосування IoT в сільському господарстві;
34. Роль IoT в охороні здоров'я;

35. Використання IoT в транспортних системах (Connected Vehicles);
36. Законодавче регулювання IoT;
37. Стандарти безпеки для IoT.

Робочу програму навчальної дисципліни (силабус) **«Основи технології Інтернету речей (IoT)»:**
Складено доц,кафедри ЦТЕ к.т.н., доц. Довженко Надією Михайлівною

Ухвалено кафедрою ЦТЕ (протокол № 21 від 30.05.2024р)
Погоджено Методичною комісією НН ІАТЕ КПІ ім. Ігоря Сікорського (протокол № 9 від 31.05.2024 р.)