



Силабус освітнього компонента

Програма навчальної дисципліни



Python для Інтернету речей (IoT)

Шифр та назва спеціальності

257 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Освітня програма

Управління інформаційною безпекою

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Профільна підготовка, Вибіркова

Семестр

8

Мова викладання

Українська

Викладачі, розробники



Погасій Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua

Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Курс "Python для Інтернету речей (IoT)" розроблений для студентів, які бажають набути навичок програмування IoT пристроїв за допомогою мови Python. В межах курсу студенти ознайомляться з базовими принципами IoT, архітектурою IoT систем, та вивчать методи підключення, обробки даних і контролю IoT пристроїв. Курс охоплює теми від основ Python до складних програмних рішень, інтегрованих з сенсорами, мережами та хмарними сервісами..

Мета та цілі дисципліни

Метою навчальної дисципліни “Python для Інтернету речей (IoT)”, забезпечити студентів теоретичними знаннями та практичними навичками розробки програмного забезпечення для Інтернету речей з використанням мови Python.

Цілі курсу: Навчити основ програмування на Python для управління IoT пристроями. Ознайомити з основними принципами та архітектурою IoT систем. Надати практичний досвід створення додатків для IoT з використанням сенсорів, мереж та хмарних сервісів. Розвинути вміння обробляти та аналізувати дані, зібрані з IoT пристроїв.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-7. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.

ФК-1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

ФК-8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.

ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки

ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

ПРН-17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 24 год., лабораторні роботи – 12 год., самостійна робота – 54 год.

Передумови вивчення дисципліни (пререквізити)

Безпека інтернет-речей, Основи програмування.

Особливості дисципліни, методи та технології навчання

Викладання дисципліни передбачає використання пояснювально-ілюстративного та репродуктивного методів, а також активізацію навчально-пізнавальної діяльності через презентації, індивідуальні та групові проекти, моделювання систем, майстер-класи

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до Інтернету речей (IoT) та Python.

Основи IoT: архітектура, компоненти та використання. Роль Python у розробці IoT рішень

Тема 2. Основи програмування на Python.

Огляд Python: типи даних, управління потоками, функції. Використання бібліотек Python у розробці IoT.

Тема 3. Робота з апаратним забезпеченням.

Основні платформи для IoT: Raspberry Pi, Arduino. Підключення та програмування датчиків

Тема 4. Модулі Python для IoT.

Модулі для роботи з сенсорами та периферійними пристроями (RPi.GPIO, Adafruit). Робота з датчиками через Python.

Тема 5. Протоколи зв'язку для IoT.

Протоколи передачі даних: HTTP, MQTT, CoAP. Підключення IoT пристроїв до Wi-Fi

Тема 6. Робота з сенсорами та актуаторами.

Типи сенсорів: температури, вологості, світла, руху. Управління актуаторами через Python (реле, двигуни)

Тема 7. Основи роботи з мережею у Python.

Огляд хмарних платформ для IoT (AWS, Google Cloud, Azure). Відправлення даних у хмару

Тема 8. Інтеграція IoT-пристроїв з хмарними сервісами.

Задачі оптимізації у машинному навчанні. Градієнтний спуск та методи прискорення оптимізації (метод Ньютона, моментум)

Тема 9. Реалізація асинхронних задач у Python.

Асинхронне програмування (asyncio). Приклади для ефективного обробки даних IoT

Тема 10. Поточкова передача даних з IoT.

Організація поточкових даних з IoT пристроїв. Використання WebSocket та інших поточкових протоколів

Тема 11. Безпека в IoT.

Основи безпеки мережеских протоколів для IoT. Шифрування даних та автентифікація пристроїв

Тема 12. IoT-проекти на Python.

Огляд успішних IoT-проектів. Планування і реалізація IoT-системи.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Налаштування середовища розробки для IoT на Python.

Тема 2. Основи програмування на Python для IoT.

Тема 3. Робота з мікроконтролерами на Python.

Тема 4. Реалізація протоколу HTTP у Python.

Тема 5. Застосування протоколу MQTT для IoT.

Тема 6. Реалізація асинхронного програмування.

Тема 7. Управління актуаторами через Python.

Тема 8. Програмування систем реального часу на Python.

Тема 9. Реалізація безпечного підключення IoT-пристроїв.

Тема 10. Моніторинг та обробка IoT даних через хмарні сервіси.

Тема 11. Реалізація проекту IoT на Python.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: <http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/>

Погодження

Силабус погоджено

28.08.2024



Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП
Роман КОРОЛЬОВ