Силабус освітнього компонента
Програма навчальної дисципліни

Python для Інтернету речей (IoT)

Шифр та назва спеціальності
125 – Кібербезпека та захист інформаці)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Кібербезпека

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–2. Знання та розуміння предметної області та розуміння професії.
КЗ–5. Здатність до пошуку, оброблення та аналізу інформації.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Результати навчання

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних

інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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 ефективної обробки даних IoT
Тема 10. Потокова передача даних з IoT.
Організація потокових даних з IoT пристроїв. Використання WebSocket та інших потокових протоколів
Тема 11. Безпека в IoT.
Основи безпеки мережевих 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.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
Python 2, Exploring IoT with Cisco Packet Tracer (5)
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література

1. Васильєв О.М., Програмування мовою Python. – Тернопіль:Навчальна книга – Богдан, 2019. URL: https://books.google.com.ua/books/about/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BC%D0%BE%D0%B2%D0%BE%D1%8E_Py.html?id=11hcEAAAQBAJ&redir_esc=y
2. Костюченко А.О., Основи програмування мовою Python:навчальний посібник. – Чернігів, ФОП Баликіна С.М. 2020. URL: https://epub.chnpu.edu.ua/jspui/bitstream/123456789/5584/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%BC%D0%BE%D0%B2%D0%BE%D1%8E%20Python.pdf
3. David Mertz, Functional Programming in Python. – O'Reilly Media,2015. URL: https://pepa.holla.cz/wp-content/uploads/2016/10/functional-programming-python.pdf

Додаткова література

4. Introduction to IoT (Cisco Networking Academy) // Електронний ресурс. Режим доступу: https://www.netacad.com.
5. IoT Fundamentals Big Data & Analytics (Cisco Networking Academy) //Електронний ресурс. Режим доступу: https://www.netacad.com.
6. Python data analysis library // Електронний ресурс. Режим доступу: https://pandas.pydata.org
7. Z. Shelby, K.Hartke, and C. Bormann, The Constrained Application Protocol (CoAP). RFC 7252, 2014. [Online]. Available: http://www.rfc-editor.org/info/rfc7252. Accessed on: June 1, 2018.

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
Сергій ЄВСЕЄВ