



Силабус освітнього компонента

Програма навчальної дисципліни



Python для інтернет-речей

Шифр та назва спеціальності

K4 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Спеціалізація**Кафедра**

Кібербезпеки (328)

Освітня програма

Управління інформаційною безпекою

Тип дисципліни

Вибіркова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна

Семестр

8

Мова викладання

Українська

Викладачі, розробники

**ПОГАСІЙ Сергій Сергійович**

Serhii.Pohasii@khpi.edu.ua

Доктор технічних наук, доцент, професор 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. Гарант освітньо-наукової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, 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 заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК7. 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.

СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.

СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.

Результати навчання

РН3. 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.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

РН17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отримання несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

РН22. 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 – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Безпека інтернет-речей, Основи програмування.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до IoT та Python. Основи програмування Python для IoT. Основи Інтернету речей: архітектура, компоненти, сфери застосування. Роль Python у розробці IoT-рішень, переваги використання мови у роботі з датчиками та пристроями. Типи даних, управління потоками, функції, бібліотеки Python. Практичні приклади застосування для розробки IoT-систем.	2
Тема 2. Робота з апаратним забезпеченням та сенсорами. Основні платформи IoT (Raspberry Pi, Arduino). Підключення та програмування датчиків і актуаторів через Python. Використання модулів RPi.GPIO, Adafruit для керування периферійними пристроями.	2
Тема 3. Протоколи та мережеві технології IoT. Протоколи передачі даних HTTP, MQTT, CoAP. Підключення IoT-пристроїв до Wi-Fi. Основи потокової передачі даних та відправлення інформації в хмару (AWS, Google Cloud, Azure).	2
Тема 4. Асинхронне програмування та обробка даних. Використання Python asyncio для асинхронної обробки даних. Потокова обробка IoT-пристроїв, оптимізація швидкодії та управління великими обсягами даних у реальному часі.	2
Тема 5. Безпека та проєкти IoT. Основи безпеки IoT: шифрування, автентифікація пристроїв, захист мережевих протоколів. Планування, реалізація та приклади успішних IoT-проєктів на Python.	2
Загальна кількість годин	10

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1 Налаштування середовища та основи Python для IoT. Встановлення Python, IDE та бібліотек для IoT. Основи синтаксису Python, типи даних, умови, цикли, функції.	3	0,1
Тема 2. Робота з мікроконтролерами та сенсорами. Підключення та програмування мікроконтролерів (Raspberry Pi, Arduino). Читання даних з датчиків та керування периферійними пристроями.	3	0,1

Тема 3. Протоколи передачі даних для IoT. Використання HTTP та MQTT для обміну даними між пристроями. Публікація, підписка та робота з брокером MQTT.	3	0,1
Тема 4. Асинхронне програмування та управління актуаторами. Асинхронна обробка даних у Python (asyncio). Керування реле, двигунами, світлодіодами та іншими актуаторами.	3	0,1
Тема 5. Безпека та хмарні сервіси для IoT. Шифрування даних, автентифікація пристроїв. Відправлення та обробка IoT-даних через хмарні платформи (AWS, Google Cloud, Azure).	4	0,1
Тема 6. Реалізація та оптимізація IoT-проекту. Планування, розробка та тестування IoT-проекту на Python. Оптимізація коду та масштабування систем для великої кількості пристроїв.	4	0,1
Загальна кількість годин	20	$\sum_{i=1}^m a_i=0,6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Розробка IoT-системи на Python із використанням сенсорів та хмарних сервісів. Демонстрування знання основ Python для IoT, підключення мікроконтролерів і сенсорів, збір та обробку даних, використання протоколів передачі даних (HTTP, MQTT), управління актуаторами, застосування асинхронного програмування, а також відправку та обробку даних через хмарні сервіси. Практична реалізація IoT-проекту, оцінку безпеки передавання даних та звіт із результатами тестування системи.	0,2
Загалом	$\sum_{i=1}^m b_i=0,2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Обробка даних сенсорів у реальному часі. Методи фільтрації та агрегації даних, обробка сигналів, відстеження аномалій у показниках сенсорів.	10
Тема 2. Використання баз даних для IoT. Збереження та отримання даних IoT-пристроїв у SQL і NoSQL базах, оптимізація структури даних для швидкого доступу.	11
Тема 3. Візуалізація IoT-даних. Використання бібліотек Matplotlib, Seaborn, Plotly для створення графіків та дашбордів із даних сенсорів.	11
Тема 4. Реалізація віддаленого управління IoT-пристроями. Створення серверів і клієнтів для дистанційного управління актуаторами через HTTP/MQTT, інтеграція з мобільними додатками.	11

Тема 5. Протоколи безпеки та шифрування в IoT. Методи автентифікації пристроїв, шифрування даних, використання TLS/SSL для безпечної передачі інформації.	11
Загальна кількість годин	54

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Introduction to IoT»
<https://www.netacad.com/courses/iot>
2. Онлайн-курс CISCO «Python for IoT»
<https://developer.cisco.com/learning/tracks/iot/python-iot>
3. Онлайн-курс CISCO «IoT Device Management»
<https://developer.cisco.com/learning/tracks/iot/device-management>

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Євсєєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсєєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. –120 с.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.
2. Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : <https://docs.python.org/3/>.
3. Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : <https://docs.oracle.com/javase/8/docs/>.
4. Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : <https://docs.microsoft.com/en-us/cpp/?view=msvc-170>

Додаткова література

1. Python Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/python/index.htm>.
2. Java Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/java/index.htm>.
3. ++ Tutorial [Електронний ресурс]. – Режим доступу : <https://www.tutorialspoint.com/cplusplus/index.htm>.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,4	0,2		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I ,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої O з округленням до найближчого цілого числа в більшу сторону.

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

Здобувач вищої освіти 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

30.08.2025



Завідувач кафедри

Сергій ЄВСЕЄВ

30.08.2025



Гарант ОП

Роман КОРОЛЬОВ