СИЛАБУС ДИСЦИПЛІНИ
«Основи Інтернету речей»

Ступінь вищої освіти – Бакалавр
Спеціальність 121, 122, 123, 125
Освітня програма «Кібербезпека»
Рік навчання 3, семестр 6
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор курсу	 **Коваленко Олексій Єпифанович, професор, д.т.н. (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж і кібербезпеки, корпус. 15, к. 207, тел. +38-044-5278724** **e-mail** o.kovalenko@nubip.edu.ua
Сторінка курсу в eLearn	**ЕНК:** https://elearn.nubip.edu.ua/course/view.php?id=4707

ОПИС ДИСЦИПЛІНИ

Дисципліна «Основи Інтернет речей» є вибірковою дисципліною навчального плану бакалаврів з спеціальностей галузі знань 12 «Інформаційні технології» і відіграє важливу роль у підготовці фахівців з інформаційних технологій.

Метою навчальної дисципліни «Основи інтернету речей» є забезпечення базової підготовки студентів в галузі архітектури сучасних комп'ютерних систем Інтернету речей, процесорів, периферійного обладнання та функціональної організації і взаємодії апаратного і програмного забезпечення; розуміння основних тенденцій розвитку та фундаментальні принципи функціонування Інтернету речей, ознайомлення студентів з технологічними і архітектурними основами побудови сучасних IoT систем.

Завдання навчальної дисципліни «Основи Інтернету речей» – вивчення основ організації та використання засобів інтернету речей (Internet of Things – IoT) у комп'ютерних системах та мережах, дослідження проблем конфігурування, аналізу, управління, забезпечення ефективного використання систем інтернету речей в організаціях і на підприємствах різних напрямків діяльності та різних форм власності.

ФАХОВІ КОМПЕТЕНТНОСТІ ТА ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

Програмні результати навчання (ПРН):

ПРН 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;

ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

ПРН 12. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;.

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема	**Години** (лекції/ лабораторні,)	**Результати навчання**	**Завдання**	**Оцінювання, %**
1 семестр				
Модуль 1. Основи архітектури інтернету речей				
Тема 1. Вступ до Інтернету речей.	**2/2**	Вміти знаходити інформацію про основи Інтернету речей, знати тенденції розвитку розумних речей і їх роботу в Інтернет.	Захист лабораторної роботи	**20**
Тема 2. Архітектура інтернету речей.	**4/4**	Вміти визначати архітектуру систем Інтернету речей на основі рекомендацій стандартів.	Захист лабораторної роботи.	**20**
Тема 3. Сенсори та актуатори інтернету речей	**4/4**	Вміти застосовувати аналогові та цифрові датчики, що використовуються в IoT системах, здійснювати їх налагодження та програмувати..	Захист лабораторної роботи.	**30**
Тема 4. Мережні протоколи інтернету речей	**4/4**	Вміти застосовувати знання для розв'язування задач для налагодження міжмашинної взаємодії за допомогою стандартизованих протоколів обміну даними. Застосовувати сучасні методи керування пристроями у IoT мережах.	Захист лабораторної роботи.	**30**
Разом за змістовим модулем 1	**14/14**			**100**

Модуль 2. Основи організації функціонування інтернету речей				
Тема 1. Комп'ютерні засоби граничних обчислень інтернету речей	**4/4**	Вміти застосовувати знання для побудови компонентів граничної області Інтернету речей.	Захист лабораторної роботи.	**20**
Тема 2. Платформи та шлюзи інтернету речей	**4/4**	Вміти застосовувати знання для розв'язування завдань для налагодження вибору платформ та налагодження шлюзів Інтернету речей.	Захист лабораторної роботи.	**30**
Тема 3. Основи організації безпеки в системах інтернету речей	**4/4**	Вміти обробляти та аналізувати мережевий трафік у IoT мережах.	Захист лабораторної роботи.	**30**
Тема 4. Основи розробки систем інтернету речей	**4/4**	Вміти застосовувати знання для визначення функцій та вимог до побудови цільових систем Інтернету речей	Захист лабораторної роботи.	**20**
Разом за змістовим модулем 2	**16/16**			**100**
Всього за семестр	**30/30**			**70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, за станом здоров'я).
Політика щодо академічної доброчесності:	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Самостійні роботи, реферати повинні мати коректні текстові посилання на використані джерела інформації.
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись за індивідуальним графіком (в он-лайн формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання**	
	екзаменів	**заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. ЕНК «Introduction to IoT» академії Cisco https://www.netacad.com/courses/iot/introduction-iot
2. ЕНК «Data Analytics Essentials» академії Cisco https://skillsforall.com/course/data-analytics-essentials?courseLang=en-US

3. ЕНК «Introduction to Architecting Smart IoT Devices» освітнього порталу Coursera https://www.coursera.org/learn/iot-devices
4. Жураковський Б. Ю., Зенів І.О. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.
5. Сторчак К.П., Тушич А.М., Срібна І.М., Яковенко Н.Д., Кравець Д.В. Технології Інтернет речей. Навч. посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ, 2021. – 68 с.
6. ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture, 2018. URL: https://www.iso.org/standard/65695.html.
7. ENISA. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017
8. Вимірювальні перетворювачі (сенсори): підручник / В. М. Ванько, Є. С. Поліщук, М. М. Дорожовець та ін. ; за ред. Є. С. Поліщука ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2015. – 584 с
9. Коваленко О.Є. Конвергенція інтернету речей та систем ситуаційного управління. Математичні машини і системи. 2023. № 3. С. 89–103. DOI: 10.34121/1028-9763-2023-3-89-103
10. Коваленко О.Є. Моделі безпеки інтернету речей. Математичні машини і системи. 2023. № 4. С. 43–50. DOI: 10.34121/1028-9763-2023-4-43-50
11. IoT technologies and protocols. URL: https://azure.microsoft.com/en-us/solutions/iot/iot-technology-protocols/
12. What is Matter? Explaining the World's Latest Smart Home Protocol. URL: https://homey.app/en-us/wiki/what-is-matter/
13. A Comparison of IoT Routers: Speed, Range, and Compatibility URL: https://firstsourcewireless.com/blogs/blog/a-comparison-of-iot-routers-speed-range-and-compatibility
14. What is an IoT Gateway (Complete Guide 2023): Definition, Examples, Functions URL: https://www.dusuniot.com/blog/what-is-an-iot-gateway/
15. Global Industrial IoT Platforms: Reviews and Ratings. URL: https://www.gartner.com/reviews/market/global-industrial-iot-platforms
16. Industrial IoT Platforms: What You Need to Know from the Gartner Magic Quadrant 2020. URL: https://www.record-evolution.de/en/blog/the-industrial-iot-platform-insights-from-the-gartner-magic-quadrant-2020/
17. IoT Development. Top 15 Internet of Things Tools and Platforms in 2023 URL: https://www.sam-solutions.com/blog/iot-development/
18. Ontologies for the Internet of Things. DOI: 10.1145/2093190.2093193 URL: https://www.researchgate.net/publication/254004296
19. HOW TO DEVELOP AN APP FOR THE INTERNET OF THINGS (IOT). URL: https://nix-united.com/blog/how-to-develop-an-app-for-the-internet-of-things-iot/
20. IoT-Lite Ontology. URL: https://www.w3.org/Submission/iot-lite/
21. Lakshmibai T. Sensors and actuators. - https://kanchiuniv.ac.in/wp-content/uploads/2021/05/BMTF183T60-SENSORS-AND-ACTUATORS-1.pdf