Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра комп'ютерних систем та мереж

"ЗАТВЕРДЖУЮ"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____**Петро ШПАТАР**
"31" березня 2026 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

ВК11 IoT розумних будівель і міст
(назва навчальної дисципліни)

вибіркова
(вказати: обов'язкова / вибіркова)

Освітньо-професійна програма Комп'ютерна інженерія
(назва програми)

Спеціальність F7 Комп'ютерна інженерія
(вказати: код, назва)

Галузь знань F Інформаційні технології
(вказати: шифр, назва)

Рівень вищої освіти другий (магістерський)
(вказати: перший бакалаврський/другий магістерський)

фізико-технічних та комп'ютерних наук
(назва факультету/ навчально-наукового інституту,
на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання українська

Чернівці 2026 рік

Робоча програма навчальної дисципліни «IoT розумних будівель і міст» складена відповідно до освітньо-професійної програми «Комп'ютерна інженерія».

Розробник: Олар Оксана Яремівна, доцент кафедри КСМ, канд. техн. наук, доцент

(П.І.Б. авторів, посада, науковий ступінь, вчене звання)

Викладач (чі), що забезпечує читання даної навчальної дисципліни:
Олар Оксана Яремівна, доцент кафедри КСМ, канд. техн. наук, доцент

(П.І.Б. викладача (ів), посада, науковий ступінь, вчене звання)

Затверджено на засіданні кафедри *комп'ютерних систем та мереж*

Протокол № 2 від "31" серпня 2026 року

Завідувач кафедри _____ **Георгій ВОРОБЕЦЬ**
(підпис)

Схвалено методичною радою навчально-наукового інституту фізико-технічних та комп'ютерних наук

Протокол № 1/2 від "31" серпня 2026 року

Голова методичної ради навчально-наукового інституту фізико-технічних та комп'ютерних наук

_____ **Іван КОЗЯРСЬКИЙ**
(підпис)

1. Мета навчальної дисципліни

Мета: формування необхідного рівня теоретичної і практичної підготовки студентів для грамотного використання ними знань про принципи IoT та смарт технології, а також про їх застосування у розумних будівлях і містах, що є необхідним при вивченні суміжних дисциплін та у майбутній професійній діяльності; для досягнення мети студентам надаються систематизовані знання про елементи та функції розумного будинку, автоматизацію пристроїв, кібербезпеку розумних будівель, а також концепції архітектури розумного міста, інформаційні технології та інформаційно-технологічні платформи.

2. Результати навчання

Вивчення навчальної дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗК - загальних

ЗК1. Здатність до адаптації та дій в новій ситуації.

ЗК3. Здатність проводити дослідження на відповідному рівні.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

СК – фахових (спеціальних)

СК2. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

СК7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.

СК9. Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їхніх компонентів.

СК12. Здатність вирішувати завдання комп’ютерної інженерії з використанням апаратно-програмної обробки даних, засобів штучного інтелекту, хмарних технологій, Інтернету речей та комп’ютеризованих інформаційно-вимірювальних систем і комплексів.

РН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.

РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп’ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення складних задач комп’ютерної інженерії та дотичних проблем.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп’ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

РН13. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань інформаційних технологій і дотичних міжгалузевих питань до фахівців і нефахівців, зокрема до осіб, які навчаються.

РН14. Розробляти високоефективні комп’ютерні системи з використанням сучасних апаратних засобів, зокрема, мікроконтролерів, мікрокомп’ютерів, програмованих логічних інтегральних схем, багатоядерних процесорів.

Знати: базове програмування для підтримки пристроїв IoT, елементи й функції розумного будинку й особливості автоматизації пристроїв, загрози й атаки розумного будинку та забезпечення безпеки; архітектурні концепції IoT для розумних міст, моделі, апаратні засоби та сучасні технології й стандарти розумного міста; інформаційні технології та інформаційно-технологічні платформи.

Вміти: проектувати безпечний розумний будинок, визначати пристрої IoT і здійснювати керування ними в розумному будинку, забезпечувати функцію збору інформації за допомогою давачів та інтелектуальних засобів, застосовувати IoT для рішень автоматизації будівель та забезпечувати конфіденційність даних необхідними інструментами кібербезпеки; вміти визначати архітектурні концепції інтернету речей для розумних міст, поєднувати апаратні засоби й технології розумного будинку відповідно до вимог та стандартів.

3. Опис навчальної дисципліни
3.1. Загальна інформація

Форма навчання	Рік підготовки	Семестр	Кількість		Кількість годин						Вид підсумкового контролю
			кредитів	всього годин	лекції	практичні	семінарські	лабораторні	самостійна робота	індивідуальні завдання	
Денна	1(5)	1(9)	4	90	16	-	-	16	58	-	Залік
Заочна	1(5)	1(9)	4	90	4	-	-	4	82	-	Залік

3.2. Структура змісту навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Інтернет речей та розумні технології												
Тема 1. Сучасний стан та перспективи розвитку IoT у розумних будівлях і містах	4	2	-	2	-	7	12	0,5	-	1	-	10,5
Тема 2. Елементи, структура та функції розумної будівлі	4	2	-	2	-	7	11	0,5	-	1	-	9,5
Тема 3. Застосування IoT для автоматизації та управління будинками	4	2	-	2	-	7	11	0,5	-	1	-	9,5
Тема 4. Кібербезпека у розумних будинках	4	2	-	2	-	8	11	0,5	-	0	-	10,5
Разом за змістовим модулем 1	45	8	-	8	-	29	45	2	-	3	-	40
Змістовий модуль 2. Архітектура розумного міста та її застосування на основі IoT												
Тема 5. Концепція, моделі та технології розумного міста	4	2	-	2	-	7	12	0,5	-	1	-	10,5
Тема 6. Мережеві архітектури та протоколи зв’язку в	4	2	-	2	-	7	11	0,5	-	1	-	9,5

системах розумного міста												
Тема 7. Обчислювальна інфраструктура розумного міста на основі IoT	4	2	2	2	-	7	11	0,5	-	1	-	9,5
Тема 8. Реалізація концепції розумного міста в Україні та світі	4	2	-	2	-	6	11	0,5	-	0	-	10,5
Разом за змістовим модулем 2	45	8	2	8	-	27	45	2	-	3	-	40
Усього годин	90	16	2	16	-	56	90	4	-	6	-	80

Тематика лекційних занять з переліком питань

№	Назва теми з основними питаннями
1	**Сучасний стан і перспективи розвитку IoT у розумних будівлях і містах.** Розгляд основних понять та принципів Інтернету речей (IoT). Сучасні тенденції, сфери застосування та перспективи розвитку IoT у розумних будівлях і містах. Приклади впровадження IoT-рішень.
2	**Елементи, структура та функції розумної будівлі.** Поняття та основні компоненти розумної будівлі. Датчики, виконавчі пристрої, контролери та системи моніторингу й управління. Основні функції та принципи взаємодії компонентів розумної будівлі.
3	**Застосування IoT для автоматизації та управління будинками.** Технології IoT для автоматизації освітлення, опалення, вентиляції, кондиціонування та енергоспоживання. Використання датчиків і систем керування для підвищення енергоефективності, комфорту та безпеки. Приклади автоматизованих систем розумного будинку.
4	**Кібербезпека у розумних будинках.** Основні загрози інформаційній безпеці IoT-систем. Основні принципи забезпечення кібербезпеки розумних будинків.
5	**Концепція, моделі та технології розумного міста.** Поняття, основні характеристики та складові розумного міста. Моделі побудови інтелектуальної міської інфраструктури та застосування IoT у транспорті, енергетиці, екологічному моніторингу й господарстві. Сучасні технології цифровізації міського середовища.
6	**Мережеві архітектури та протоколи зв'язку в системах розумного міста.** Принципи побудови мереж IoT та рівні їхньої архітектури. Основні протоколи

	передавання даних і бездротового зв’язку, зокрема MQTT, CoAP, Wi-Fi, Bluetooth Low Energy, Zigbee та LoRaWAN. Особливості вибору технологій зв’язку залежно від вимог до дальності, енергоспоживання та швидкості передавання даних.
7	**Обчислювальна інфраструктура розумного міста на основі IoT.** Архітектура обчислювальної інфраструктури IoT та принципи обробки даних від міських сенсорних систем. Використання хмарних і периферійних обчислень (Cloud Computing і Edge Computing), платформ зберігання та аналізу даних. Інтеграція інформаційних систем для моніторингу й управління міською інфраструктурою.
8	**Реалізація концепції розумного міста в Україні та світі.** Міжнародний досвід упровадження технологій розумного міста та приклади успішних проєктів. Сучасний стан цифровізації міської інфраструктури в Україні, основні досягнення й проблеми. Перспективи розвитку українських розумних міст на основі IoT, інтелектуальних систем управління та цифрових платформ.

3.3. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин
1	Інтернет речей у системах розумного будинку та міста (Семінар)	2
2	Проєктування мережі розумного будинку та програмування IoT-пристроїв (Лабораторна робота № 1)	4
3	Автоматизація розумного будинку за допомогою мережі Wi-Fi (Лабораторна робота № 2)	4
4	Дослідження розумного міста (Лабораторна робота № 3)	2
5	Оцінювання ризиків в IoT-системі (Практична робота)	4
	Разом	16

3.4. Самостійна робота студента

№	Назва теми/ кількість балів/ форма контролю	Кількість годин
1	Взаємодія IoT з перспективними інформаційно-комунікаційними технологіями / результати використовуються при виконанні презентації № 1 (6 балів)	8
2	Зниження енергоспоживання в розумних будівлях і містах / результати використовуються при виконанні лабораторної роботи № 1 (6 балів)	6

3	Рішення IoT для автоматизації систем розумних будівель / результати використовуються при виконанні лабораторної роботи № 2 (6 балів)	8
4	Загрози та кібератаки на розумні будівлі / результати використовуються при виконанні тесту 1 (6 балів) та модульної контрольної роботи (МКР) № 1 (6 балів)	8
5	Технології, що використовуються в розумних містах / результати використовуються при виконанні лабораторної роботи № 3 (8 балів)	6
6	Стандарти ISO / IEEE для розумних міст / результати використовуються при виконанні тесту 2 (8 балів)	6
7	Аналіз ризиків і загроз безпеці в системах IoT розумних будівель і міст / результати використовуються при виконанні практичної роботи (8 балів)	8
8	Технології розумних міст / результати використовуються при виконанні МКР № 2 (6 балів)	6
	Разом	56

4. Форми і методи навчання

Основними формами організації навчання є лекційні та лабораторні заняття, а також самостійна робота здобувачів вищої освіти. Самостійна робота спрямована на опрацювання матеріалів лекцій та літературних джерел.

У процесі вивчення дисципліни застосовуються такі методи навчання:

- Пояснювально-ілюстративний метод – виклад теоретичного матеріалу з використанням прикладів схем, діаграм, таблиць і мультимедійних презентацій для пояснення основних понять, принципів і методологій.
- Демонстраційний метод – показ прикладів розробки та реалізації комп’ютерних систем.
- Практичний метод – виконання лабораторних завдань, спрямованих на формування навичок роботи з апаратно-програмними засобами комп’ютерних систем.
- Проблемно-пошуковий метод – постановка практичних проблем і ситуацій, пов’язаних розробкою та застосуванням комп’ютерних систем.
- Аналіз практичних ситуацій – розгляд прикладів побудови комп’ютерних систем для вирішення прикладних завдань із застосуванням мікроконтролерів, мікрокомп’ютерів та комп’ютерних кластерів.
- Обговорення та навчальні дискусії – колективний аналіз проблемних питань, обговорення результатів виконання лабораторних робіт, порівняння можливих підходів до побудови комп’ютерних систем.
- Презентація результатів виконаних завдань – представлення та захист розроблених програмних моделей комп’ютерних систем, обґрунтування прийнятих рішень і формулювання висновків.

Застосовуються інноваційні освітні технології, зокрема, інформаційно-комунікаційні та студентоцентрованого навчання. Освітні технології передбачають використання мультимедійних матеріалів для лекційних занять, методичних вказівок для виконання лабораторних робіт, мов та середовищ розробки комп'ютерних програм, комп'ютерної та телекомунікаційної техніки, відеоконференцій, системи електронного навчання Moodle з метою розвитку навичок аналізу, розробки та використання комп'ютерних систем штучного інтелекту.

5. Система контролю та оцінювання

Система контролю та оцінювання передбачає перевірку рівня засвоєння теоретичних знань, сформованості практичних умінь і здатності застосовувати цифрові інструменти для виконання навчальних завдань. Оцінювання здійснюється систематично протягом семестру з урахуванням своєчасності, самостійності, правильності та якості виконаних робіт.

Форми та методи контролю

***Поточний контроль*:** *усне опитування* студента на лекційних заняттях (фронтальне, індивідуальне); *письмовий контроль* (звіти із виконання лабораторних робіт); *практичний контроль* (захист лабораторних робіт); *тестовий/машинний контроль* (тести у системі Moodle).

Рубіжний контроль: письмові контрольні роботи у кінці змістових модулів №1 і №2.

Підсумковий контроль – залік.

6. Критерії оцінювання поточного та підсумкового контролю

Поточне оцінювання (аудиторна та самостійна робота)									**Підсумковий контроль (залік)**	**Сумарна кількість балів**
Змістовий модуль 1					**Змістовий модуль 2**					
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
6	6	6	6	6	8	8	8	6	40	100

Т1, Т2 ... Т15 – теми змістових модулів; М1, М2, М3 – модульні контрольні роботи

Залежно від характеру відповіді здобувача освіти зазначена кількість балів може бути скоригована за наступними критеріями:

К-ть балів	**Критерії оцінки**
max	здобувач освіти дає вичерпну відповідь на поставлене запитання;
0,8 · max	здобувач освіти при відповіді на поставлене запитання припустився незначних неточностей, які не впливають на суть відповіді;

0,6 · max	здобувач освіти при відповіді на поставлене запитання припустився помилок, які виправляє за допомогою викладача; в середньому може дати правильні відповіді на 50% питань теми;
0,4 · max	здобувач освіти при відповіді на поставлене запитання припустився суттєвих помилок, які все ж таки виправляє за допомогою викладача; дає правильні відповіді на 30% питань теми;
0,2 · max	отримує здобувач освіти, який за допомогою викладача фрагментарно відповідає на запитання, проте не в повній мірі володіє мінімальним рівнем знань з даного питання;
0	якщо характер відповідей дає підставу стверджувати, що здобувач освіти неправильно зрозумів суть питання чи не знав правильної відповіді, а тому відповідав, припускаючись грубих помилок.

Примітка: за max прийнято максимальну оцінку для даного виду діяльності. Заокруглення проводиться до одиниць балу.

Згідно шкали ECTS загальна кількість балів, яку здобувач освіти може отримати у процесі вивчення дисципліни, становить 100 балів, з яких 60 балів здобувач освіти набирає при поточних видах контролю і 40 балів – у процесі підсумкового контролю (залік).

Шкала оцінювання: національна та ЄКТС

Оцінка за національною шкалою	**Оцінка за шкалою ECTS**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим повторним курсом

7. Перелік питань для самоконтролю та підсумкового контролю навчальних досягнень здобувачів освіти

Змістовий модуль 1. Інтернет речей та розумні технології

1. Що таке Інтернет речей (IoT) та які його основні принципи?
2. Які основні компоненти формують архітектуру IoT-системи?
3. Які переваги надає використання IoT у розумних будівлях і містах?
4. Які перспективні інформаційно-комунікаційні технології взаємодіють з IoT?
5. Які основні тенденції та перспективи розвитку IoT у міській інфраструктурі?

6. Що таке розумна будівля та які її основні функції?
7. Які датчики використовуються в системах розумної будівлі та які параметри вони вимірюють?
8. Яке призначення контролерів і виконавчих пристроїв у системах автоматизації будівель?
9. Які системи життєзабезпечення та інженерні системи можуть інтегруватися в розумну будівлю?
10. Які принципи взаємодії між IoT-пристроями забезпечують автоматизоване управління будівлею?
11. Які завдання можна автоматизувати за допомогою IoT у розумному будинку?
12. Як організувати проєктування мережі розумного будинку з урахуванням вимог до підключення IoT-пристроїв?
13. Як здійснюється програмування та налаштування IoT-пристроїв у системах розумного будинку?
14. Які можливості надає використання Wi-Fi для автоматизації розумного будинку?
15. Як IoT використовується для автоматизації освітлення, опалення, вентиляції та кондиціонування?
16. Які основні загрози кібербезпеці існують у системах розумних будівель?
17. Які типові кібератаки можуть бути спрямовані на IoT-пристрої та мережі?
18. Які вразливості найчастіше виникають у системах Інтернету речей?
19. Які методи автентифікації, шифрування та контролю доступу застосовуються для захисту IoT-систем?
20. Як здійснюється оцінювання ризиків і визначення рівня загроз в IoT-системах розумних будівель?

Змістовий модуль 2. Архітектура розумного міста та її застосування на основі IoT

21. Що таке розумне місто та які основні складові його інфраструктури?
22. Які моделі та архітектури використовуються для побудови систем розумного міста?
23. Як IoT застосовується для управління міським транспортом, освітленням і комунальними послугами?
24. Які технології використовуються для моніторингу стану довкілля в розумному місті?
25. Які переваги та проблеми виникають під час упровадження концепції розумного міста?
26. Які рівні та компоненти охоплює мережева архітектура IoT-систем?
27. Які особливості використання Wi-Fi, Bluetooth Low Energy, Zigbee та LoRaWAN у системах IoT?
28. Для чого призначені протоколи MQTT і CoAP та в чому полягають відмінності між ними?

29. За якими критеріями обирають мережеві технології для підключення IoT-пристроїв?
30. Які основні вимоги висуваються до надійності, масштабованості та безпеки мереж розумного міста?
31. Які основні компоненти формують обчислювальну інфраструктуру розумного міста?
32. У чому полягають відмінності між хмарними та периферійними обчисленнями в IoT-системах?
33. Як здійснюються збирання, передавання, зберігання та оброблення даних від IoT-пристроїв?
34. Які інформаційно-технологічні платформи використовуються для моніторингу й управління системами розумного міста?
35. Які переваги та обмеження має використання великих даних і штучного інтелекту в міській інфраструктурі?
36. Які основні міжнародні стандарти IEEE застосовуються у сфері розумних міст?
37. Які приклади успішного впровадження технологій розумного міста відомі у світі?
38. Який сучасний стан розвитку розумних міст в Україні?
39. Які українські міста впроваджують IoT-рішення та в яких сферах вони використовуються?
40. Які основні перспективи й перешкоди розвитку розумних міст в Україні?
41. Як технології IoT сприяють зниженню енергоспоживання в розумних будівлях?
42. Які датчики та алгоритми використовуються для оптимізації освітлення, опалення й кондиціонування?
43. Як IoT допомагає підвищувати енергоефективність міської інфраструктури?
44. Які технології застосовуються для моніторингу енергоспоживання та управління енергетичними ресурсами?
45. Які показники використовують для оцінювання енергоефективності розумних будівель і міст?
46. Що таке ризик інформаційної безпеки та які основні чинники його формують в IoT-системах?
47. Які методи використовуються для ідентифікації, аналізу й оцінювання ризиків IoT?
48. Як визначити ймовірність виникнення загрози та можливі наслідки її реалізації для розумної будівлі?
49. Які технічні й організаційні заходи дають змогу зменшити ризики безпеки IoT-пристроїв?
50. Як розробити план управління ризиками для IoT-системи розумної будівлі або міста?

8. Рекомендована література
Фахова (основна)

1. National Institute of Standards and Technology (NIST). 2021. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST Special Publication 800-213. DOI [Електронний ресурс] – https://doi.org/10.6028/NIST.SP.800-213
2. National Institute of Standards and Technology (NIST). 2024. The Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. DOI [Електронний ресурс] – https://doi.org/10.6028/NIST.CSWP.29
3. European Union Agency for Cybersecurity (ENISA). 2024. ENISA Threat Landscape 2024. [Електронний ресурс] – https://www.enisa.europa.eu/publications
4. United Nations Human Settlements Programme (UN-Habitat). 2022. World Cities Report 2022: Envisaging the Future of Cities. Nairobi: UN-Habitat. [Електронний ресурс] – https://unhabitat.org/wcr/
5. International Energy Agency (IEA). 2024. Energy Efficiency 2024. Paris: International Energy Agency. [Електронний ресурс] – https://www.iea.org/reports
6. International Organization for Standardization (ISO). 2022. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva: ISO. [Електронний ресурс] – https://www.iso.org/standard/27001
7. International Organization for Standardization (ISO). 2022. ISO/IEC 27400:2022 Cybersecurity – IoT Security and Privacy – Guidelines. Geneva: ISO. [Електронний ресурс] – https://www.iso.org/
8. International Organization for Standardization (ISO). 2021. ISO 37106:2021 Sustainable Cities and Communities – Guidance on Establishing Smart City Operating Models for Sustainable Communities. Geneva: ISO. [Електронний ресурс] – https://www.iso.org/
9. Cisco Networking Academy. 2026. Cisco Packet Tracer. [Електронний ресурс] – https://www.netacad.com/courses/packet-tracer
10. 10. OASIS Open. 2025. MQTT: The Standard for IoT Messaging. [Електронний ресурс] – https://mqtt.org/
11. Bluetooth Special Interest Group (Bluetooth SIG). 2025. Bluetooth Core Specification. [Електронний ресурс] – https://www.bluetooth.com/specifications/
12. European Telecommunications Standards Institute (ETSI). 2025. ETSI Standards for Internet of Things and Cybersecurity. [Електронний ресурс] – https://www.etsi.org/standards
13. Institute of Electrical and Electronics Engineers (IEEE). 2021–2026. IEEE Xplore Digital Library: Research Publications on Internet of Things, Smart Buildings and Smart Cities. [Електронний ресурс] – https://ieeexplore.ieee.org/
14. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О.

Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.

15. Богуслав А.М. Методи та моделі забезпечення захисту безпроводних сенсорних мереж// електрон. текст. Дані URL: http://er.nau.edu.ua/bitstream/NAU/22464/2/diser_ua_2.0.pdf
16. John Blyler 8 Critical IoT Security Technologies // електрон. текст. Дані URL: https://www.electronicdesign.com/industrial-automation/8-critical-iot-security-technologies
17. Security in the internet of things // електрон. текст. дані URL: Sehttps://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_securityin-the-internet-of-things.pdf
18. Wolfgang Apolinarski, Umer Iqbal, and Josiane Xavier Parreira. 2014. The GAMBAS mid-dleware and SDK for smart city applications. In Pervasive Computing and Communica-tions Mas - sive IoT Data. In Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. 324-327.DOI [Електронний ресурс] – http://dx.doi.org/10.1109/SOCA.2014.47
19. Luis Sanchez, Luis Muoz, Jose Antonio Galache, Pablo Sotres, Juan R. Santana, Veronica Gutierrez, Ra-jiv Ramdhany, Alex Gluhak, Srdjan Krco, Evangelos Theodoridis, and Dennis Pfisterer. 2014. Smart-Santander: IoT experimentation over a smart city testbed. Computer Networks 61 (2014), 217 – 238. DOI [Електронний ресурс] – http://dx.doi.org/10.1016/j.bjp.2013.12.020

Допоміжна

20. Sylva Girtelschmid, Matthias Steinbauer, Vikash Kumar, Anna Fensel, and Gabriele Kotsis. 2013. Big Data in Large Scale Intelligent Smart City Installations.In Proceedings of International Conference on Infor- mation Integration and Web-based Applications & Services (IIWAS ’13). ACM, New York, NY, USA, Article428, 5 pages. DOI [Електронний ресурс] – http://dx.doi.org/10.1145/2539150.2539224
21. Giseppe Piro, Ilaria Cianci, Luigi A. Grieco, Gennaro Boggia, and Pietro Camarda. 2014. Informa- tion centric services in Smart Cities. Journal of Systems and Software 88, 0 (2014), 169 – 188. DOI [Електронний ресурс] – http://dx.doi.org/10.1016/j.jss.2013.10.029
22. Yong Woo Lee and Seungwoo Rho. 2010. U-city portal for smart ubiquitous middleware. In Advanced Com- munication Technology (ICACT), 2010 The 12th International Conference on, Vol. 1. 609–613. 30. Wolfgang Apolinarski, Umer Iqbal, and Josiane Xavier Parreira. 2014. The GAMBAS middleware and SDK for smart city applications. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on. 117– 122. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/PerComW.201 4.6815176
23. Flix J. Villanueva, Maria J. Santofimia, David Villa, Jess Barba, and Juan Carlos Lopez. 2013. Civ- itas: The Smart City Middleware, from Sensors to Big Data. In Innovative Mobile and Inter- net Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on. 445–450. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/IMIS.2013.80

24. Junping Qiu, Yanhui Song, and Siluo Yang. 2010. Digital Integrated Model of Government Resources under E-Government Environment. In Internet Technology and Applications, 2010 International Conference on. 1–4. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/ITAPP.2010.5566315
25. Levent Gurgen, Ozan Gunalp, Yazid Benazzouz, and Mathieu Gallissot. 2013. Self-aware cyber-physical systems and applications in smart buildings and cities. In Design, Automation Test in Europe Conference Exhibition (DATE), 2013. 1149–1154. DOI [Електронний ресурс] – http://dx.doi.org/10.7873/
26. Gilles Privat, Mengxuan Zhao, and Laurent Lemke. 2014. Towards a Shared Software Infrastructure for Smart Homes, Smart Buildings and Smart Cities. In International Workshop on Emerging Trends in the Engineering of Cyber-Physical Systems, Berlin. 35. Jiafu Wan, Di Li, Caifeng Zou, and Keliang Zhou. 2012. M2M Communications for Smart City: An Event- Based Architecture. In Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. 895–900. DOI [Електронний ресурс] – http://dx.doi.org/10.1109/CIT.2012.188
27. Riccardo Petrolo, Valeria Loscri, and Nathalie. Automation Test in Europe Conference Exhibition (DATE), 2013. 1149–1154. DOI [Електронний ресурс] – http://dx.doi.org/10.7873/DATE.2013.240
28. Jean-Paul Calbimonte, Sofiane Sarni, Julien Eberle, and Karl Aberer. 2014. XGSN: An Open-source Semantic Sensing Middleware for the Web of Things. In 7th International Workshop on Semantic Sensor Networks.
29. Danh Le-Phuoc, Hoan Quoc Nguyen-Mau, Josiane Xavier Parreira, and Manfred Hauswirth. 2012. A mid- dleware framework for scalable management of linked streams. Web Semantics: Science, Services and Agents on the World Wide Web 16 (2012), 42–51.

9. Інформаційні ресурси

1. Навчальна платформа Moodle. URL: https://moodle.chnu.edu.ua/course/view.php?id=2620
2. Освітні програми кафедри КСМ – URL: https://csn.chnu.edu.ua/about-us/ok-rivni/
3. ОПП «Комп'ютерна інженерія» (магістратура). URL: https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/

10. Політика академічної доброчесності

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ЧНУ:

- «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/etychnyi-kodeks-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/

- «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-zapobihannia-akademichnomu-plahiatu-u-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/
- «Політика використання штучного інтелекту в Чернівецькому національному університеті імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polityka-vykorystannia-shtuchnoho-intelektu-v-chernivetskomu-natsionalnomu-universyteti-imeni-yuriia-fedkovycha/

Використання здобувачами освіти інструментів штучного інтелекту (ШІ) під час виконання навчальних завдань:

- допускається за умови дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої роботи, а у разі використання ШІ зобов'язаний зазначити факт і спосіб його застосування);
- не допускається використання ШІ як заміни самостійного виконання завдань або з метою порушення вимог академічної доброчесності;
- додаткові обмеження чи вимоги щодо використання ШІ можуть визначатися викладачем в освітньому процесі для конкретних видів навчальної діяльності відповідно до особливостей дисципліни.