СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Технології IoT та блокчейн
Мова викладання	українська
Викладач	Петренко Тарас Анатолійович, доцент
Профайл викладача	Сайт кафедри: https://mmi.stu.cn.ua/personal-kafedry/ Google академія: https://scholar.google.com/citations?user=2bJE-4IAAAAJ&hl=ru
Контакти викладача	тел.: 0636419136, e-mail: mail_taras@ukr.net

1. Анотація курсу - створення та використання технологій блокчейн та «Інтернету речей» залишається складною теоретичною й технічною проблемою. Необхідність у їх використанні виникає в самих різних областях – у військової справі й системах безпеки країни, економічних системах, системах моніторингу та управління містами, у системах «Розумний дім» та повсякденній діяльності людини.

На заняттях курсу «Технології IoT та блокчейн» студенти отримують теоретичні знання та практичні вміння в сфері проектування, впровадження, безпечної експлуатації та супроводження систем Smart City та розумний дім. Знайомляться з технологією блокчейн і криптовалют. Розглядають концепцію Інтернету речей та блокчейн, їх складові та застосування у світі та в Україні. Досліджують проблеми безпеки які потрібно вирішити при створенні рішень для IoT. Проводять наукові дослідження в зазначених напрямках.

2. Мета та цілі курсу - формування науково-професійного світогляду магістра спеціальності 125 – Кібербезпека в області використання технологій IoT та блокчейн для захисту інформації та в повсякденній професійній діяльності. Формування у студентів фундаментального розуміння суті технологій Інтернету речей та блокчейн, переваг їх використання в інформаційних системах та кібербезпеці. Засвоєння основ розробки та програмування пристроїв, які працюють з використанням смарт-технологій та технологій «Інтернету речей». При цьому пристрої IoT розглядаються як сукупність технічних, інформаційних та програмних засобів, призначених для вирішення широкого кола завдань у різних галузях економіки, освіти, промисловості тощо.

Під час вивчення дисципліни здобувач вищої освіти має набути або розширити наступні загальні та фахові компетентності, передбачені освітньою програмою:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 4. Здатність розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного

класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій.

КФ 9. Здатність розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

Основними завданнями вивчення дисципліни "Технології IoT та блокчейн" є:

– ознайомлення з сучасним станом та тенденціями розвитку проблеми впровадження технологій IoT та блокчейн;

– практичне ознайомлення з особливостями та засвоєння основ роботи з пристроями, датчиками та засобами комунікації «Інтернету речей».

– вивчення механізмів безпеки блокчейн технологій і використання криптовалют;

– оволодіння студентами теоретичними основами роботи стеку протоколів при взаємодії компонентів IoT систем;

– набуття студентами практичних навичок використання протоколів передачі даних в IoT системах;

– формування у студентів стійких знань щодо архітектури побудови систем IoT;

– формування навичок забезпечувати безпеку використання і протидію правопорушенням, пов'язаними із криптовалютами;

3. Результати навчання:

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання, передбачені освітньою програмою:

ПРН 2. планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

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 5. реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 7. проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв'язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо ;

ПРН 8. проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН10. розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно - апаратних комплексів, підсистем, програмного

забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;

ПРН14. розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

Після вивчення дисципліни «Технології IoT та блокчейн» ЗВО повинні:

знати :

– основи побудови блокчейн технології, принципи побудови, проведення та затвердження трансакцій криптовалюти; принципи побудови і функціонування розумних контрактів.

– призначення, еволюцію та класифікацію смарт-технологій та сфери Інтернету речей;

– принципи побудови пристроїв IoT, їх переваги та недоліки;

– призначення та основи моделі взаємодії пристроїв IoT та відповідних веб-платформ;

– сучасні тенденції розвитку смарт-технологій;

– основні напрямки розвитку та ключові технологічні рішення проектів IoT;

– базові принципи розробки пристроїв IoT.

– принципи роботи протоколів передачі даних в IoT системах, стек протоколів,

– сфери та специфіку використання протоколів передачі даних в IoT системах.

вміти :

– використовувати технології IoT та блокчейн при проектуванні інформаційних систем в різних сферах діяльності;

– забезпечувати безпеку IoT та блокчейн технологій під час їх проектування, впровадження та експлуатації;

– забезпечувати взаємодію компонентів IoT систем на основі протоколів передачі даних;

– проектувати IoT системи, що передбачають використання протоколів передачі даних.

– використовувати теоретичні знання під час розв'язання практичних задач, пов'язаних з побудовою та налагодженням пристроїв галузі Інтернету речей;

– налаштовувати мережеву взаємодію між пристроями IoT через Ethernet, Bluetooth та інші мережі;

– використовувати сучасні середовища розробки додатків на основі технології блокчейн (проект Ethereum).

налаштовувати хмарні сервіси для підтримки роботи пристроїв IoT;

– аналізувати технічні характеристики функціональних вузлів пристрої IoT;

– здійснювати пошук оптимальних рішень при побудові пристроїв IoT та інформаційних систем на основі смарт-технологій.

4. Обсяг курсу. 4 кредитів ECTS, що становить 120 годин роботи студентів, з них 90 годин самостійної роботи та 30 годин аудиторної роботи з викладачем.

Вид заняття	Загальна кількість годин
Лекції	16
Лабораторні заняття	14
Самостійна робота (РГР, наукові дослідження)	90

Тематика курсу

Змістовий модуль 1. Технологія Internet Of Things

1. Основні поняття та базові принципи технології IoT
2. Інформаційно-вимірювальні технології IoT
3. Передавання інформації в каналах IoT
4. Сенсори IoT
5. Перетворення сигналів IoT
6. Мережеві технології IoT
7. Взаємодія Arduino з роботами і системами розумний дім
8. Плата WiFi ESP8266 в проектах Arduino
9. Мікрокомп'ютер Raspberry PI 3 для Інтернету речей
10. Хмарні сервіси IoT
11. Проблеми безпеки розвитку технології IoT

Змістовий модуль 2. Технологія blockchain

12. Теоретичні основи технології блокчейн
13. Технологія блокчейн і криптовалюти
14. Принципи технології Blockchain
15. Алгоритми доказу виконаної роботи
16. Мережа Bitcoin
17. Проект Ethereum
18. Безпека та надійність технології Blockchain

5. Пререквізити. Передумовою для вивчення курсу «Технології IoT та блокчейн» є успішне засвоєння дисциплін: інформатика, архітектура комп'ютерних систем, комп'ютерна схемотехніка, технології програмування, комп'ютерні мережі, основи криптографічного захисту інформації, методи побудови та аналізу криптосистем та ін. Дисципліна «Технології IoT та блокчейн» є базовою для подальшої успішної професійної діяльності за спеціальністю, а також може використовуватися під час підготовки випускної кваліфікаційної роботи магістра.

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	ECTS
Вимоги розрахунково-графічної роботи	При перевірці та оцінюванні розрахунково-графічної роботи враховується правильність виконання теоретичних та практичних завдань, самостійність виконання, вчасність здачі роботи та відповідність оформлення результатів діючим вимогам
Лабораторні заняття	Кожна виконана лабораторна робота оцінюється від 0 до 3-х балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок студента за темою, самостійності виконання роботи та вчасності її захисту
Умови допуску до підсумкового контролю	Умовою допуску до екзамену є виконання та отримання хоча б мінімальної кількості балів з усіх обов'язкових видів навчальної роботи передбачених робочою програмою (лабораторних, модульного контролю та розрахунково-графічної роботи). Мінімальна кількість балів необхідна для допуску до екзамену – 20.

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів	
Змістовий модуль 1. Технологія Internet Of Things			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	6
2	Підготовленість до лабораторних робіт. Рівень знань студента за темою лабораторної роботи (максимум - 2 бали за кожну лаб. роботу)	0	14
3	Самостійність виконання лабораторних робіт (максимум 0,5 бала)	0	3,5
4	Своєчасність виконання лабораторних робіт (максимум 0,5 бала)	0	3,5
5	Поточний модульний контроль	0	10
Змістовий модуль 2. Технологія Blockchain			
1	Повнота ведення конспектів занять (присутність на лекції+конспект – 1 бал за кожну лекцію)	0	4
2	Підготовленість до лабораторних робіт. Рівень знань студента за темою лабораторної роботи (максимум - 2 бали за кожну лаб. роботу)	0	6
3	Самостійність виконання лабораторних робіт (максимум 0,5 бала)	0	1,5
4	Своєчасність виконання лабораторних робіт (максимум 0,5 бала)	0	1,5
Оцінка за РГР		**0**	**10**
Семестрова оцінка поточного контролю		**0**	**60**
Екзамен		**0**	**40**

Шкала оцінювання: національна та ECTS

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
			для екзамену, КСР, КП, ДР	для заліку
Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, проводить наукові дослідження	90 – 100	**A**	відмінно	зараховано
Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	82-89	**B**	добре	
Студент вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом	75-81	**C**		

викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок				
Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих	66-74	**D**	задовільно	
Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	60-65	**E**		
Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	0-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

7. Політики курсу.

7.1 Академічна доброчесність – самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності – академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Національного університету «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26 за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження оцінювання (контрольна робота, іспит, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми; відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту); позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати навчання.

7.2 Політика дедлайнів – своєчасність здачі лабораторної роботи оцінюється в 0,5 бала за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 2 бали. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

7.3 Політика перезарахування кредитів у випадку мобільності – перезарахування відбувається якщо назви навчальних дисциплін ідентичні або мають незначну стилістичну відмінність, але обсяги та змістова частина навчальних програм не відрізняються; кількість кредитів, відведена на вивчення навчальної дисципліни відрізняється менше, ніж на 25 %; форми підсумкового контролю з дисциплін однакові. При перезарахуванні дисципліни зберігається раніше здобута позитивна оцінка. Перескладання іспиту з дисципліни з метою підвищення оцінки, визначеної в

документах виданих здобувачу вищої освіти за попереднім місцем навчання, не дозволяється. Перезарахування кредитів проводиться відповідно до Порядку визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка» Затв. Вченою радою НУ «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26.

7.4 Політика щодо відвідування – відвідування занять є обов'язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

7.5 Політика щодо правил поведінки на заняттях – активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв тільки для навчання.

7.6 Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

8. Рекомендована література та інформаційні джерела

1. Cisco академія. [Електронний ресурс]. – Режим доступу: http://edu-cisco.org
2. Drescher, Daniel. Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, 2017.
3. Hanes D. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. 1st ed. Cisco Press, 2017. 576 p.
4. Khan, R. [and others], Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT), 2012 10th International Conference on. — 2012. — 257-260 с.
5. Prometheus: Платформа масових відкритих онлайн-курсів [Електронний ресурс]. – Режим доступу: https://prometheus.org.ua
6. Raspberry Pi 3 Model B / Raspberry Pi Community. [Електронний ресурс] – Режим доступу: https://www.raspberrypi.org/products/raspberry-pi-3-model-b
7. Грінгард С. Інтернет речей / пер. з англ. Харків: Клуб сімейного дозвілля, 2018. 176 с.
8. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. - М.: НИЦ ИНФРА-М, 2015. - 200 с.
9. Магда Ю.С. Raspberry Pi Руководство по настройке и применению — М.: ДМК пресс, 2014 — 188с.
10. Могильний С. Б. Покрокова побудова системи для Інтернету речей // Вісник Національного технічного університету України "Київський політехнічний інститут". Серія : Радіотехніка. Радіоапаратобудування. - 2016. - Вип. 65. - С. 73-78.
11. Орлюк Є. А. Розробка системи "Розумний Будинок" на базі "arduino" / Є. А. Орлюк // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. – Електрон. текст. дані. – 2018

12. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.
13. Соколов М.Н., Смолянинова К.А., Якушина Н.А. Проблемы безопасности интернета вещей: обзор. — Вопросы кибербезопасности : журнал. — 2015. — №5(13). — 34с.
14. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
15. Технології проектування систем IoT [Електронний ресурс]. – Режим доступу: https://elearn.nubip.edu.ua/enrol/index.php?id=1577