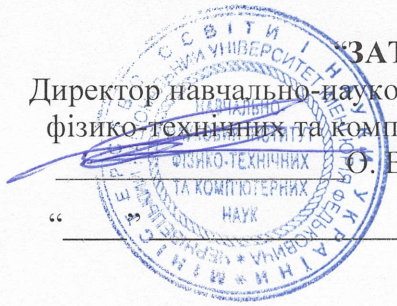
Чернівецький національний університет імені Юрія Федьковича
(повне найменування закладу вищої освіти)

Навчально-науковий інститут фізико-технічних та комп'ютерних наук
(назва навчально-наукового інституту / факультету)

Кафедра комп'ютерних систем та мереж



"ЗАТВЕРДЖУЮ"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ О. В. Ангельський
"____" _____ 2022 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

Технологія IoT Blockchain
(назва навчальної дисципліни)

вибіркова
(вказати: обов'язкова / вибіркова)

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

Спеціальність 123 Комп'ютерна інженерія
(вказати: код, назва)

Галузь знань 12 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 2022 рік

Робоча програма навчальної дисципліни

Технологія IoT Blockchain

(назва навчальної дисципліни)

складена відповідно до освітньо-професійної програми

Комп'ютерна інженерія, 123 Комп'ютерна інженерія,

(назва освітньо-професійної програми, код та назва спеціальності)

12 Інформаційні технології, 15 квітня 2021 р.

(галузь знань: шифр та назва; дата останнього затвердження)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ,
канд. техн. наук, асистент

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

Погоджено з гарантом ОП і затверджено на засіданні кафедри
комп'ютерних систем та мереж

Протокол № 1 від "29" серпня 2022 року

Завідувач кафедри _____ *(Воробець Г.І.)*
(підпис) (прізвище та ініціали)

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

Протокол № 1 від "31" серпня 2022 року

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

_____ (Струк Я. М.)
(підпис) (прізвище та ініціали)

1. Мета навчальної дисципліни

Мета: надання студентам міждисциплінарних знань для побудови системи міжмашинної взаємодії пристроїв Інтернету речей та створення машинно-машинної (M2M) економіки – що, по суті, є обміном грошима між пристроями і вилучення людини із процесу їх взаємодії і функціонування.

Вивчення даної вибіркової дисципліни надає студентам ряд переваг, оскільки матеріал курсу допоможе при аналізі інформаційних джерел, підготовці магістерських робіт, статей, доповідей на науково-практичних конференціях. Окрім цього, засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування комплексної системи захисту інформації, в тому числі комерційного характеру.

2. Результати навчання

У результаті вивчення навчальної дисципліни студент отримує компетентності, у результаті чого повинен

2.1. Знати: найновіші досягнення в галузі інформаційної безпеки банківського бізнесу, наявні існуючі системи здійснення мікроплатежів, системи міжмашинної взаємодії (M2M), основи технології блокчейн, принципи формування блокчейн-мереж, основи побудови захищених систем Інтернету речей та мереж блокчейн, контроль та моніторинг цих систем.

2.2. Вміти: будувати системи Інтернету речей із врахуванням вимог кібербезпеки для їх подальшого масштабування та підвищення продуктивності для побудови машинно-машинної (M2M) економіки - цифрових грошей для мікротранзакцій; обирати для проектування криптовалютні проекти, орієнтованих на індустрію Інтернету речей; будувати розподілені мережі Інтернету речей для керування, моніторингу та управління; забезпечувати підвищений рівень захисту побудованих систем.

2.3. Набути компетентностей:

ЗК - загальних

ЗК3. Здатність проводити дослідження на відповідному рівні.

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

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

СК – фахових (спеціальних)

СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.

СК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.

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.

СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

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

ПРН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.

РН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

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.

РН7. Вирішувати задачі аналізу та синтезу комп'ютерних систем та мереж.

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

3. Опис навчальної дисципліни
3.1. Загальна інформація

Назва навчальної дисципліни *Технологія IoT Blockchain*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсум-кового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	**1(5)**	**1(9)**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Залік**
Заочна	**1(5)**	**1(9)**	**4**	**120**	**2**	**4**	**-**	**-**	**4**	**112**	**-**	**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. Блокчейн та Інтернет речей (IoT)												
Тема 1. Вступ. Основні поняття побудови екосистеми Інтернету речей.	14	2	-	2	-	10	14	1	-	1	-	12
Тема 2. Аналіз моделі загроз для системи IoT	14	2	-	2	-	10	14	0	-	-	-	14
Тема 3. Основи технології блокчейн	14	2	-	2	-	10	16	1	-	1	-	14
Тема 4. Система блокчейн для побудови машинно-машинної (M2M) економіки.	14	2	-	2	-	10	16	0	-	-	-	16
Разом за змістовим модулем 1	56	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Механізми захисту мереж Інтернету речей												
Тема 5. Захист Інтернету речей на рівні пристроїв.	19	2	-	2	-	15	20	1	-	1	-	18
Тема 6. Захист Інтернету речей на рівні комунікацій.	19	2	-	2	-	15	18	0	-	-	-	18
Тема 7. Захист Інтернету речей на рівні додатків.	26	3	-	3	-	20	22	1	-	1	-	20
Разом за змістовим модулем 2	64	7	-	7	-	50	60	2	-	2	-	56
Усього годин	120	15	-	15	-	90	120	4	-	4	-	112

3.5. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин
1.	Дослідження IoT системи розумний дім	2
2.	Налаштування міжмашинної взаємодії в IoT системі	2
3.	Моделювання загроз на рівні пристроїв Інтернету речей	2
4.	Моделювання загроз на комунікаційному рівні IoT	2
5.	Моделювання загроз на прикладному рівні IoT	3
6.	Моделювання загроз для оцінки ризиків у системі IoT	3
7.	Побудова захищеної системи мікроплатежів IoT-системи за допомогою блокчейн	3
	Разом	15

3.7. Самостійна робота студента (ІНДЗ – індивідуальне навчально-дослідне завдання)

№	Назва теми/ кількість балів/ форма контролю	Кількість годин
1	Чому блокчейн потребує масштабування? / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1 (5 балів)	10
2	Стейкінг (Proof of Stake) / результати використовуються при виконанні модульної контрольної роботи (МКР) № 1 (5 балів)	10
3	Майнінг (Proof of Work) / результати використовуються при виконанні лабораторної роботи № 1 (5 балів)	10
4	Блокчейн та розподілені файлові системи / результати використовуються при виконанні лабораторної роботи № 2 (5 балів)	10
5	Анатомія атаки IoT / результати використовуються при виконанні МКР № 2 (5 балів)	15
6	Моделі контролю доступу / результати використовуються при виконанні МКР № 2 (5 балів)	15
7	Керування ідентифікацією пристроїв IoT / результати використовуються при виконанні МКР № 2 (5 балів)	20
	Разом	90

4. 4. Методи навчання

Для викладання матеріалів з навчальної дисципліни «Технологія IoT Blockchain» використовуються наступні методи навчання.

4.1. Словесні методи навчання. Навчальна лекція

За допомогою даного методу забезпечується усне викладення матеріалу великими ємністю й складністю логічних побудов, доказів і узагальнень. В ході лекції використовуються прийоми усного викладення інформації, підтримання уваги протягом тривалого часу, активізації мислення студентів, прийоми забезпечення логічного запам’ятовування, переконання, аргументації, доказів, класифікації, систематизації і узагальнення. В залежності від специфіки лекційного матеріалу іноді використовується лекція-діалог.

4.2. Індуктивний метод навчання

Даний метод навчання використовується в рамках лекційних занять, коли матеріал носить, здебільшого, фактичний характер. В рамках лабораторних занять метод застосовується при виконанні технічних задач, коли студенти використовують раніше здобуті теоретичні знання при роботі з конкретними пристроями (комп’ютерами) та програмними продуктами.

4.3. Репродуктивний метод навчання

Даний метод навчання використовується в рамках лекційних і лабораторних занять, а також під час самостійної роботи студентів. Метод передбачає роботу студентів за визначеним алгоритмом. Згідно з методом для виконання завдань студентам надаються методичні вказівки, правила і навчальні приклади.

4.4. Проблемно-пошукові методи навчання

Проблемно-пошукові методи застосовуються в ході проблемного навчання, а саме в процесі виконання лабораторних робіт та індивідуальних науково-дослідних завдань. Слід зауважити, що під проблемною ситуацією треба вважати невідповідність між тим, що вивчається і вже вивченим. При використанні проблемно-пошукових методів навчання викладач використовує такі прийоми: створює проблемну ситуацію (ставить питання, пропонує задачу, експериментальне завдання), організує колективне обговорення можливих підходів до рішення проблемної ситуації, стимулює висування гіпотез, тощо. Студенти роблять припущення про шляхи вирішення проблемної ситуації, узагальнюють раніше набуті знання, виявляють причини явищ, пояснюють їхнє походження, вибирають найбільш раціональний варіант вирішення проблемної ситуації. Викладач обов'язково керує цим процесом на всіх етапах, а також за допомогою запитань-підказок. Також даний метод використовується при опрацюванні матеріалів в системі дистанційної освіти «Moodle» та в мережній академії «Cisco».

4.5. Наочний метод навчання

Наочний метод достатньо важливий для студентів, оскільки забезпечує візуальне подання навчального матеріалу, зокрема, з використанням інформаційно-комунікаційних технологій. При викладанні дисципліни наочний метод навчання поєднується зі словесними методами для представлення інформації у вигляді таблиць, рисунків, схем та діаграм.

5. Критерії оцінювання результатів навчання з навчальної дисципліни

Шкала оцінювання: національна та ЄКТС (Європейська кредитна трансферно-накопичувальна система, ECTS)

Оцінка за національною шкалою (залік)	**Оцінка за шкалою ЄКТС**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Зараховано	A (90-100)	Зараховано
	B (80-89)	
	C (70-79)	
	D (60-69)	
	E (50-59)	
Не зараховано	FX (35-49)	Не зараховано з можливістю повторного складання
	F (1-34)	Не зараховано з обов'язковим повторним вивченням дисципліни

6. Засоби оцінювання

Засобами оцінювання та демонстрування результатів навчання є

- контрольні роботи;
- стандартизовані тести;
- презентації результатів виконаних завдань та досліджень;
- завдання на лабораторному обладнанні.

7. Форми поточного та підсумкового контролю

Формами поточного контролю рівня знань є усна та письмова відповідь студента при захисті виконаних лабораторних робіт, кількість отриманих балів при виконанні тестового завдання, а також письмова відповідь при написанні модульних контрольних робіт.

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Підсумковий тест (залік)	Сума балів
Змістовий модуль 1					Змістовий модуль 2				30	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
5	5	5	5	10	10	10	10	10		

Т1, Т2 ... Т7 – теми змістових модулів; М1, М2 – модульні контрольні роботи

Підсумковий контроль (**залік**) – 30 балів: здійснюється виконання фінальної контрольної роботи на курсі Академії CISCO IoT Fundamentals: IoT Security.

8. Рекомендована література

Фахова (основна)

1. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.
2. IoT maturity in the new digital world URL: https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Get-smart-about-data-integration-for-a-truly-smart-city
3. IT Strategy Headquarters. «E-Japan Strategy» January 22, 2001 URL: https://japan.kantei.go.jp/it/network/0122full_e.html
4. Яцків Н. Г. Перспективи використання технології блокчейн у мережі інтернет речей . Науковий вісник НЛТУ України. 2016. Вип. 26.8. С. 381-387. [Електронний ресурс]. URL: http://nbuv.gov.ua/UJRN/nvnltu_2016_26.

Допоміжна

1. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку. Вісник Національного університету "Львівська політехніка". 2014. № 806 : Комп'ютерні системи та мережі. С. 154–161.
2. Наконечний А.Й., Верес З.Є. Інтернет речей і сучасні технології. Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування. 2016. № 852.С. 136-138.
3. Roundup Of Internet Of Things Forecasts 2017. [Electronic resource]. URL: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-thingsforecasts/#77a4556b1480.

9. Інформаційні ресурси

1. https://csn.chnu.edu.ua/about-us/ok-rivni/
2. https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/

3. Cisco -Україна. Режим доступу:: https://www.cisco.com
4. Annual Threat Reports. Режим доступу:: https://www.fireeye.com/current- threats/annual-threat-report.html
5. European union agency for cybersecurity. Режим доступу:: https://www.enisa.europa.eu
6. IoT Fundamentals: IoT Security. Інтернет-ресурс Академії CISCO, Режим доступу: https://www.netacad.com/courses/cybersecurity/iot-security