

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"

Заступник керівника
(проректор з науково-педагогічної роботи)



Микола АФАНАСЬСВ

ОСНОВИ РОЗРОБКИ ДЕЦЕНТРАЛІЗОВАНИХ ЗАСТОСУВАНЬ (DECENTRALIZED APPLICATIONS (DAPPS))

робоча програма навчальної дисципліни

Галузь знань *12 Інформаційні технології*
Спеціальність *125 Кібербезпека*
Освітній рівень *перший (бакалаврський)*
Освітня програма *Кібербезпека*

Статус дисципліни *вибіркова*
Мова викладання, навчання та оцінювання *українська*

Завідувач кафедри
кібербезпеки та
інформаційних технологій

Сергій БВСЕБ

Харків
2020

ЗАТВЕРДЖЕНО

на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:

Корольов Р.В., к.т.н. доц.кафедри КІТ.

**Лист оновлення та перезатвердження
робочої програми навчальної дисципліни**

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Дисципліна “Основи розробки децентралізованих застосувань (Decentralized Applications (dapps)) ” є навчальною дисципліною з циклу професійної підготовки вільного вибору (мейджор) за спеціальністю “Кібербезпека”.

Принципи та архітектуру Bitcoin можна застосувати для вирішення широкого класу задач: від голосування і взаєморозрахунків і до управління ланцюгами поставок товарів. Блокчейн як спосіб спільної обробки інформації стає інструментом, який дозволяє проектувати надійні і прозорі облікові системи.

Предметом навчальної вивчення навчальної дисципліни є теоретичні концепції, принципи функціонування, розробки та застосування до комплексних децентралізованих застосувань (Dapps).

Мета – навчальної є засвоєння теоретичних основ та отримання практичних навичок з проектування, розробки, розгортання децентралізованих застосувань (Dapps).

Результатом вивчення дисципліни є освоєння принципів розробки, кодування, розгортання і виконання розумних (смарт) контрактів – обчислювального елементу технології blockchain.

Характеристика навчальної дисципліни

Курс	4
Семестр	8
Кількість кредитів ECTS	5
Форма підсумкового контролю	залік

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Комплексні системи захисту інформації	Дипломний проект
Організація та інформаційне забезпечення управлінської діяльності	
Менеджмент інформаційної безпеки	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17. забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних

	<p>системах;</p> <p>РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;</p> <p>РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);</p> <p>РН–25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;</p> <p>РН–26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;</p> <p>РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;</p> <p>РН–29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;</p> <p>РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації;</p> <p>РН–35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;</p> <p>РН–42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і\або кібербезпеки;</p> <p>РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;</p> <p>РН–44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;</p> <p>РН–45. застосовувати рині класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–47. вирішувати задачі захисту інформації, що обробляється в</p>
--	--

	<p>інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p>	<p>РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;</p> <p>РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p> <p>РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;</p> <p>РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;</p> <p>РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;</p> <p>РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p> <p>РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p> <p>РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно</p>

	<p>встановленої політики інформаційної і\або кібербезпеки; РН–41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і\або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати рині класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН–31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН–36 виявляти небезпечні сигнали технічних засобів; РН–37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН–38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН–39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН–40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН–47 вирішувати задачі захисту інформації, що обробляється в</p>

	інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; PH-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
--	---

Програма навчальної дисципліни

Змістовий модуль 1. Децентралізація в інформаційних системах

Тема 1. *Поняття децентралізації для інформаційних систем*

Тема 2. *Принципи роботи Bitcoin*

Тема 3. *Високорівнева архітектура Bitcoin*

Тема 4. *Введення в криптографію та управління ключами*

Змістовий модуль 2. Технологічні деталі функціонування Bitcoin

Тема 5. *Структура транзакції*

Тема 6. *Підходи до синхронізації з мережею і SPV-вузли*

Тема 7. *Механізм комісії в Bitcoin*

Тема 8. *Технологія Blockchain*

Тема 9. *Розвиток децентралізованих технологій*

Тема 10. *Конфіденційність користувачів в відкритих системах*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

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 лекції, презентації, бесіди.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- проводити розрахунок знаходження гешу блокчейн-функції;
- вміння перевіряти валідність номерів банківських карток при виконанні транзакцій смарт-контрактів;
- вміння використовувати геш-функції у якості цифрового підпису у смарт-контрактах;
- проводити оцінку надійності цифрового підпису в смарт-контракті;
- розробляти заходи протидії загрозам при використанні смарт-контрактів;
- проводити багатовимірний аналіз даних у смарт-контрактах.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в

процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 10

Лабораторні заняття: максимальна кількість балів становить 90 (виконання лабораторних робіт – 20, захист лабораторних робіт – 42, контрольні роботи – 28), а мінімальна – 45.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Мак бал
Тема 1	<i>Аудиторна робота</i>			
	Лекція	Лекція №1 " <i>Поняття децентралізації для інформаційних систем</i> "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №1. <i>Налаштування робочого простору для дослідження функціонування децентралізованої платіжної системи</i>	виконання лабораторної роботи	2

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	Аудиторна робота			
	Лекція	Лекція №2 " <i>Принципи роботи Bitcoin</i> "	Робота на лекції	1
	Лабораторне заняття	<i>Лабораторна робота №1. Налаштування робочого простору для дослідження функціонування децентралізованої платіжної системи</i>	виконання лабораторної роботи/захист лабораторної роботи	7
	Лабораторне заняття	<i>Лабораторна робота №2. Аналіз функціонування децентралізованої платіжної системи Bitcoin. Дослідження методів захисту криптовалюти</i>	виконання лабораторної роботи	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	Аудиторна робота			
	Лекція	Лекція №3 " <i>Високорівнева архітектура Bitcoin</i> "	Робота на лекції	1
	Лабораторне заняття	<i>Лабораторна робота №2. Аналіз функціонування децентралізованої платіжної системи Bitcoin. Дослідження методів захисту криптовалюти</i>	виконання лабораторної роботи /захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	Аудиторна робота			
	Лекція	Лекція №4 " <i>Введення в криптографію та управління ключами</i> "	Робота на лекції	1
	Лабораторне заняття	<i>Лабораторна робота № 3. Аналіз функціонування децентралізованої платіжної системи Ethereum. Дослідження методів захисту криптовалюти</i>	виконання лабораторної роботи	2

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	Аудиторна робота			
	Лекція	Лекція №5 "Структура транзакції "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 3. Аналіз функціонування децентралізованої платіжної системи Ethereum. Дослідження методів захисту криптовалюти	виконання лабораторної роботи/захист лабораторної роботи	7
	Лабораторне заняття	Лабораторна робота № 4. Аналіз функціонування децентралізованої платіжної системи Monero. Дослідження методів захисту криптовалюти	виконання лабораторної роботи, контрольна робота	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	Аудиторна робота			
	Лекція	Лекція №6 " Підходи до синхронізації з мережею і SPV-вузли"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 4. Аналіз функціонування децентралізованої платіжної системи Monero. Дослідження методів захисту криптовалюти	виконання лабораторної роботи/захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	Аудиторна робота			
	Лекція	Лекція №7 " Механізм комісії в Bitcoin"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Робота з Truffle	виконання лабораторної роботи	2

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	Аудиторна робота			
	Лекція	Лекція №8 "Технологія Blockchain"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Робота з Truffle	виконання лабораторної роботи/захист лабораторної роботи	7
	Лабораторне заняття	Лабораторна робота 6. Знайомство з Remix-web-середовище Solidity IDE. Основи роботи з Ethereum	виконання лабораторної роботи	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	Аудиторна робота			
	Лекція	Лекція №9 "Розвиток децентралізованих технологій "	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 6. Знайомство з Remix - web-середовище Solidity IDE. Основи роботи з Ethereum	виконання лабораторної роботи/захист лабораторної роботи	8
	Самостійна робота			
		Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань	
Тема 10	Аудиторна робота			
	Лекція	Лекція №10 "Конфіденційність користувачів в відкритих системах"	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 7. Робота з MetaMask	виконання лабораторної роботи/захист	22

			лабораторної роботи, контрольна робота	
Самостійна робота				
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. Кравченко П. Блокчейн и децентрализованные системы : учеб. пособие для студ. заведений высш. образования : в 3 частях. Ч. 1 / П. Кравченко, Б. Скрябин, О. Дубинина.– Харьков, 2019. – 488 с.
2. Даннен Крис. Введение в Ethereum и Solidity. Самиздат, 2018. – 90 с
3. Кравченко П., Скрябин Б. Блокчейн и децентрализованные системы. Часть 1. Харьков: Промарт, 2018. – 400 с.
4. Лелу Лоран. Блокчейн от А до Я. Все о технологии десятилетия. М.: Эксмо, 2017. – 256 с
5. Нараян П. Блокчейн. Разработка приложений. СПб.: БХВ-Петербург, 2018. – 500 с
6. Новикова Наталья. Терминология криптовалют. Самиздат, 2018. – 23 с.
7. Равал С. Децентрализованные приложения. Технология Blockchain в действии. СПб.: Питер, 2017. – 240 с
8. Хосп Джулиан. О криптовалюте просто. Биткоин, эфириум, блокчейн, децентрализация, майнинг, ICO & Co. СПб.: Питер, 2019. — 150
9. Wanjala Peter. A Beginner's Journey to Ethereum's Smart Contracts. [Peter Namisiko Wanjala], 2018. – 189 p.
10. Vaneetvelde Kenny. Ethereum Projects for Beginners (code).Packt Publishing, 2018. – 92 p.
11. Skvorc Bruno. Learn Ethereum: The Collection. SitePoint, 2018. – 447 p.

Додаткова

12. Coindesk, What can you buy with Bitcoin, 2015.
13. L. Kehoe, D. Daltion, C. Lonowicz, T. Jankovich, Blockchain Disruptingthe Financial Services Industry?, 2015.
14. Shelkovnikov, Blockchain Enigma. Paradox. Opportunity, 2016.
15. M. Morisse, Cryptocurrencies and Bitcoin: Charting the Research Land-scape, in: Americas Conference on Information Systems, pp. 1–16.
16. J. Manyika, C. Roxburgh, The great transformer: The impact of theInternet on economic growth and prosperity, McKinsey Global Institute(2011) 1–10.
16. G. O. Karame, E. Androulaki, S. Capkun, Double-spending fast pay-ments in bitcoin, Proceedings of the 2012 ACM conference on Computerand communications security. (2012).
17. F. Glaser, L. Bezenberger, Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems, in: European Conference on Infor-mation Systems, 57, pp. 1–18.

Інформаційні ресурси.

18. Buterin. A next-generation smart contract and decentralized application platform, 2014. <https://github.com/ethereum/wiki/wiki/White-Paper>. Accessed June 2018.

19. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Основи розробки децентралізованих застосувань (decentralized applications (dapps))" <https://pns.hneu.edu.ua/course/view.php?id=5399>".