

Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. С. Жуковського
«Харківський авіаційний інститут»

Кафедра «Інженерії програмного забезпечення» (№ 603)

ЗАТВЕРДЖУЮ

Голова НМК



(підпис)

Д.М. Крицький
(підпис та прізвище)

« 31 » 08 2021 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптовалюти і блокчейн технології

(назва навчальної дисципліни)

Галузь знань: 10 Природничі науки, 11 Математика та статистика, 12 Інформаційні технології, 15 Автоматизація та приладобудування, 16 Хімічна та біоінженерія, 17 Електроніка та телекомунікації, 19 Архітектура та будівництво

Спеціальність: 101 Екологія, 103 Науки про Землю, 113 Прикладна математика, 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 123 Комп'ютерна інженерія, 124 Системний аналіз, 125 Кібербезпека, 151 Автоматизація та комп'ютерно-інтегровані технології, 152 Метрологія та інформаційно-вимірювальна техніка, 163 Біомедична інженерія, 172 Телекомунікації та радіотехніка, 173 Авіоніка, 193 Геодезія та землеустрій

Освітня програма: усі освітні програми за відповідними спеціальностями

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Силабус введено в дію з 01.09.2021 року

Харків – 2021 р.

Розробник: Дем'яненко В.А., ст.викладач . кафедри №603
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри інженерії програмного забезпечення (№ 603)

Протокол № 2 від « 31 » серпня 2021 р.

Завідувач кафедри д-р техн.наук., проф. (науковий ступінь та вчене звання) (підпис) І.Б. Туркін (ініціали та прізвище)

Погоджено з представником здобувачів освіти:
Представник студентського самоврядування (підпис) Колодій Д.В. (ініціали та прізвище)

1. Загальна інформація про викладача



Дем'яненко Владислав Анатолійович, старший викладач кафедри. З 2001 р викладає в Національному аерокосмічному університеті ім. Н.С. Жуковського «ХАІ».

Має 9 наукових і навчально-методичних публікацій. Викладає дисципліни «Моделі і методи захисту інформації та ПО», «Безпека програм та даних», «Об'єктно орієнтоване програмування», «Криптовалюти і блокчейн технології», «Проектування розподілених систем ЕОМ.

Напрями наукових досліджень: Криптовалюти та блокчейн технології, криптографія та безпека програмного забезпечення, інтернет речей та розумний дім.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 2 семестр.

Обсяг дисципліни:

4 кредита ЄКТС (120 годин), у тому числі аудиторних – 40 годин, самостійної роботи здобувачів – 80 години.

Форми здобуття освіти

Денна, дистанційна, дуальна.

Дисципліна – обов'язкова.

Види навчальної діяльності – лекції, практичні роботи, самостійна робота здобувача.

Види контролю – поточний, модульний та підсумковий (семестровий) контроль (іспит).

Мова викладання – українська.

Необхідні обов'язкові попередні дисципліни (пререквізити) – «Проектування ПЗ систем реального часу».

Необхідні обов'язкові супутні дисципліни (кореквізити) – немає.

3. Мета та завдання навчальної дисципліни

Мета вивчення: формування знань з використання технологій блокчейн під час обігу криптовалют та застосування смартконтрактів.

Завдання: закріплення практичних навичок та умінь застосування блокчейн платформ та криптографічних методів у блокчейн технології; аналізування ризиків створення та використан-ня криптовалют; формування та аналізування смартконтрактів.

Загальні компетентності:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність спілкуватися іноземною мовою як усно, так і письмово.

ЗК03. Здатність проведення теоретичних та прикладних досліджень на відповідному рівні.

ЗК06. Здатність удосконалювати свої навички на основі аналізу попереднього досвіду.

Фахові компетентності:

ФК01. Здатність аналізувати предметні області, формувати, аналізувати та моделювати вимоги до програмного забезпечення

ФК04. Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї в інженерії програмного забезпечення.

ФК05. Здатність оцінювати ступінь обґрунтованості застосування специфікацій, стандартів, правил і рекомендацій в професійній галузі та дотримуватися їх при реалізації процесів життєвого циклу програмного забезпечення.

ФК10. Здатність визначати мету та стратегію сталого розвитку ІС відповідно до політики в галузі сталого розвитку організації.

ФК11. Здатність забезпечувати керівництво та дозволяти використання інновацій і поліпшень, які підвищують конкурентоспроможність або ефективність. Здатність демонструвати вищому керівництву бізнес-переваги потенційних змін

Програмні результати навчання:

ПРН02. Оцінювати і вибирати методи і моделі розроблення, впровадження, супроводу програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу

ПРН03. Застосовувати базові концепції і методології моделювання інформаційних процесів у прикладній області.

ПРН04. Виявляти інформаційні потреби і класифікувати дані для проектування програмного забезпечення та встановлювати план його прийнятно-здавального тестування.

ПРН07. Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для ефективного виконання конкретних виробничих задач з програмної інженерії.

ПРН09. Обґрунтовано вибирати парадигми і мови програмування для розроблення програмного забезпечення; застосовувати на практиці засоби розроблення програмного забезпечення

ПРН14. Набувати нові наукові і професійні знання, вдосконалювати навички, прогнозувати розвиток програмних систем та інформаційних технологій.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Введення в децентралізовані системи.

Тема 1. Історія виникнення і застосування основних принципів децентралізації

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Обсяг самостійної роботи здобувачів: 5 години.

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 2. Введення в біткоіни. Принципи роботи Bitcoin

Форма занять: лекція, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Криптографія в Bitcoin

Обсяг самостійної роботи здобувачів: 5 години.

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 3. Особливості роботи Bitcoin. Як влаштований біткоіни?.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 годин.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Криптографія в Bitcoin

Обсяг самостійної роботи здобувачів: 5 години.

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 4. Технологічні деталі функціонування Bitcoin.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Основи взаємодії з інтерфейсом Bitcoin вузла
- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Змістовний модуль 2. Криптографія в децентралізованих платіжних системах

Тема 5. Криптографія в децентралізованих платіжних системах

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Основи взаємодії з інтерфейсом Bitcoin вузла

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 6. Як влаштований blockchain в Bitcoin?

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Основи взаємодії з інтерфейсом Bitcoin вузла

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 7. Зберігання та обробка ключів

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Механізми формування бази даних облікової системи Bitcoin

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 8. Застосування технології блокчейн в сучасних системах. Основні підходи до досягнення консенсусу в децентралізованих системах

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Механізми формування бази даних облікової системи Bitcoin

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Модульний контроль 1

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*
 - *Обсяг аудиторного навантаження: за необхідністю*
 - *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.*
 - *Обсяг самостійної роботи здобувачів – 5 години.*
- Підготовка до модульного контролю.

Модуль 2.

Змістовний модуль 3. Застосування технології блокчейн в сучасних системах

Тема 9. Поняття, класифікація, реалізація та особливості виконання смарт-контрактів для децентралізованих додатків.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Механізми формування бази даних облікової системи Bitcoin

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 10. Базові принципи токенизації активів. Архітектура платформи токенизації, ролі учасників і процеси, що протікають в системах обліку токенів.

Форма занять: лекція, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Вплив структури транзакцій і блоків на можливість відстеження дій користувачів в обліковій системі

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 11. Конфіденційність і анонімність в децентралізованих платіжних системах.

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 годин.

Тема практичної роботи: Вплив структури транзакцій і блоків на можливість відстеження дій користувачів в обліковій системі

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): персональний комп'ютер або ноутбук.

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Тема 12. Огляд протоколу Miblewimble

Форма занять: лекція, практична робота, самостійна робота.

Обсяг аудиторного навантаження: 2 години.

Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.

Тема практичної роботи: Вплив структури транзакцій і блоків на можливість відстеження дій користувачів в обліковій системі

- *Обсяг самостійної роботи здобувачів: 5 години.*

Опрацювання матеріалу лекцій. Формування питань до викладача.

Модульний контроль 2

- *Форма занять: написання модульної роботи в аудиторії (за рішенням лектора допускається проведення у дистанційній формі).*

- *Обсяг аудиторного навантаження: за необхідністю*

- *Обов'язкові предмети та засоби (обладнання, устаткування, матеріали, інструменти): немає.*

- *Обсяг самостійної роботи здобувачів – 5 години.*

Підготовка до модульного контролю.

5. Індивідуальні завдання

Не передбачено навчальним планом

6. Методи навчання

Словесні, наочні, практичні.

7. Методи контролю

Поточний контроль (теоретичне опитування й розв'язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0...1	8	0...8
Виконання і захист лабораторних (практичних) робіт	2...5	4	8...20
Змістовний модуль 2			
Робота на лекціях	0...1	6	0...6
Виконання і захист лабораторних (практичних) робіт	2...3	6	12...18
Модульний контроль	10...20	1	10...20
Змістовний модуль 3			
Робота на лекціях	0...1	2	0...2
Виконання і захист лабораторних (практичних) робіт	3...6	1	3...6
Модульний контроль	10...20	1	10...20
Усього за семестр			60...100

Прийнята шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка для екзамену, курсового проекту (роботи), практики
90-100	відмінно
75-89	добре
60-74	задовільно
01-59	незадовільно з можливістю повторного складання

Семестровий контроль (іспит) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних питань (кожне питання 50 балів)

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь.

Добре (75-89). Твердо знати мінімум, здати тестування та поза аудиторну самостійну роботу.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх.

9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем. Питання, що стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

10. Методичне забезпечення та інформаційні ресурси

Підручники, навчальні посібники, навчально-методичні посібники, конспекти лекцій, методичні рекомендації з проведення лабораторних робіт тощо, які видані в Університеті знаходяться за посиланням:

1. Дистанційний курс дисципліни розроблено у системі дистанційного навчання Mentor, яку впроваджено в Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ», доступ до курсу за посиланням:

<https://mentor.khai.edu/course/view.php?id=215>

2. Software Engineering Institute, <https://www.sei.cmu.edu/>

3. Спілка програмістів. <https://dou.ua/>

4. Стандарти вищої освіти України бакалавра та магістра з інженерії програмного забезпечення, <https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/121-inzheneriya-programnogo-zabezpechennya-bakalavr.pdf>, <https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/2020/11/17/121-inzheneriya-prohramnoho-zabezpechennya-mahistr.pdf>

11. Рекомендована література

Базова

1. Кравченко П. К78 Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с. : іл. 191; табл. 13; бібліогр.: 124 назв.
2. Кравченко П. К78 Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с. : рис. 256; табл. 17; бібліогр.: 78 назв.
3. Кравченко П. К78 Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків: 2020. – 305 с. : ил. 178; табл. 7; библиогр.: 145 назв..
4. Кравченко П. Теория токенизации / П. Кравченко, Б. Скрябин. –Харьков : Промарт, 2018. – 46 с.
5. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system..
6. Henderson, M. R. (2018). Private IPFS Networks. <https://mrh.io/ipfs-private-networks/>..

Допоміжна

1. Huckle S. Internet of Things, Blockchain and Shared Economy Applications / S. Huckle, R. Bhattacharya, M. White, N. Beloff // Procedia Comput. Science. – 2016. – Вид. 98. – с. 461–466..
2. У. Диффи. Первые десять лет криптографии с открытым ключом. // ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.54-74.
3. А. В. Спесивцев и др. Защита информации в персональных компьютерах. – М., Радио и связь. 1992, с.140-149.
4. В. Жельников. Криптография от папируса до компьютера. – М., АБФ, 1996.
5. Bos J. W. Elliptic curve cryptography in practice / J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow // 18th International Conference, FC 2014. – Springer Berlin Heidelberg, 2014. – P. 157–175

1. Інформаційні ресурси

1. Online Browsing Platform [Електронний ресурс]. – Режим доступу: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1>:
2. IPFS is the Distributed Web [Електронний ресурс]. – Режим доступу: <https://ipfs.io>.
6. CAP theorem [Електронний ресурс] // Wikipedia. — Режим доступу: https://en.wikipedia.org/wiki/CAP_theorem.