Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор з науково – педагогічної роботи

Олександр ГОЛОВКО

“____”_____2022 р.

Робоча програма навчальної дисципліни

«Технології блокчейн»

рівень вищої освіти перший (бакалаврський)

галузь знань 012 - Інформаційні технології

спеціальність 125- Кібербезпека

освітня програма Кібербезпека

спеціалізація

вид дисциплін обов’язкова

факультет комп’ютерних наук

2022 / 2023

2

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп`ютерних наук "28 " червня 2022 року, протокол №10

РОЗРОБНИКИ ПРОГРАМИ:
Полуяненко Микола Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних систем і технологій

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від " 23 " червня 2022 року № 10

Завідувач кафедри безпеки інформаційних систем і технологій

Сергій Рассомахін

Гарант освітньої (професійної/наукової) програми

(керівник проєктної групи) Рассомахін Сергій Геннадійович

Сергій Рассомахін

Програму погоджено методичною комісією факультету комп`ютерних наук

Протокол від "24 "червня 2022 року №9

Голова методичної комісії факультету комп`ютерних наук

Анатолій Бердников

ВСТУП

Програма навчальної дисципліни «Технології блокчейн» складена відповідно до освітньої програми «Кібербезпека» підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека».

1. Опис навчальної дисципліни

1.1. Мета навчальної дисципліни

Дисципліна має на меті: надати студентам знання необхідні для оволодіння сучасними децентралізованими технологіями розподіленого реєстру, ознайомлення з термінологією, визначеннями та основними поняттями, а також побудовою та механізмами роботи блокчейн систем.

1.2. Основні завдання дисципліни:

Основними завданнями вивчення дисципліни є:

вивчення технологій, що застосовуються у блокчейн-системах; вивчення побудови та функціонування децентралізованого розподіленого реєстру; дослідження механізмів консенсусу та інших механізмів, за допомогою яких користувачі блокчейн мережі приходять до єдиного стану; дослідження обмежень та безпеки технології блокчейн.

1.3. Кількість кредитів – 4.

1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
4-й	-й
Семестр	
7-й	-й
Лекції	
32 год.	год.
Практичні, семінарські заняття	
32 год.	год.
Лабораторні заняття	
год.	год.
Самостійна робота	
56 год.	год.
Індивідуальні завдання	
У т.ч. індивідуальні завдання (курсова робота) 20год.	

1.6. Заплановані результати навчання:

У результаті вивчення даного курсу студент повинен знати:

1. Основні відомості про блокчейн біткоіна;
2. Поняття розподіленої системи;
3. Поняття блокчейн системи;
4. Класифікацію блокчейн-систем;

5. Цілісність даних в блокчейн-системах;
6. Підписання даних;
7. Адреси та управління ключами;
8. Транзакції;
9. Блоки;
10. Децентралізовані реєстри;
11. Розгалуження;
12. Модели консенсуса;

У результаті вивчення даного курсу студент повинен уміти:

1. Розгортати тестову блокчейн мережу;
2. Досліджувати процеси, які протікають у децентралізованих системах;
3. Оцінити, на базовому рівні, вразливості механізмів, що використовуються у блокчейн-системах та пов'язані з ними ризики;
4. Провести обґрунтування щодо вибору механізмів роботи децентралізованих мереж в залежності від умов їх функціонування.

У результаті вивчення даного курсу студент повинен бути ознайомленим:
з сучасними напрямками розвитку блокчейн-технологій та практичного застосування їх можливостей.

2. Тематичний план навчальної дисципліни

Тема 1. Феномен криптовалюти.

Визначення поняття криптовалюта. Законодавче врегулювання. Переваги та недоліки використання криптовалюти. Сутність криптовалюти. Поняття майнинга. Види криптовалют.

Тема 2. Криптовалюта та зловмисники.

Найбільш поширені способи шахрайства в області криптовалют. Поняття хмарного майнинга. Основні ризики при використанні криптовалют.

Тема 3. ICO: що це і навіщо воно потрібно.

Поняття ICO. Суть ICO. Історія ICO. Регулювання ICO. Правовий статус ICO. Ризики при участі в ICO. Основні модулі програми з вивчення ICO.

Тема 4. Інвестування у криптовалюти та кіберзлочинці.

Основні інструменти інвестування. Криптотрейдинг і кіберзлочинці: загрози віртуальним заощадженням і біржам. Уразливості криптобірж. Захист користувачів біржами. Кіберзахисні рішення. Верифікація користувачів біржами.

Тема 5. Введення в технологію блокчейн і загальні поняття.

Загальне поняття блокчейну. Принцип роботи блокчейну. Основні компоненти технології блокчейн. Безпечність блокчейну. Надійність і довговічність блокчейну. Області застосування. Різновиди блокчейну.

Тема 6. Блокчейн у світі.

Blockchain 3.0. Проекти нового покоління на Blockchain 3.0.

Тема 7. Поняття подвійних витрат.

Визначення поняття «подвійні витрати». Дослідження та результати атаки 51%.

Тема 8. Протоколи на основі блокчейну. Смарт-контракти.

Визначення блокчейн-протоколу. Дослідження протоколів на основі блокчейну. Переваги та недоліки протоколів. Поняття смарт-контракт. Складові смарт-контракту. Принцип роботи смарт-контрактів. Переваги та недоліки смарт-контрактів.

Тема 9. Огляд технології блокчейн. Основні механізми функціонування.

Історична довідка появи та розвідку блокчейн технологій.

Огляд технології блокчейн: поняття розподіленої системи; поняття блокчейн-системи; класифікація блокчейн-систем (permissioned, permissionless, публічний, блокчейн, що належить консорціуму, приватний блокчейн).

Вимоги до контролю доступу: процес реєстрації користувачів, перевірки тощо; визначені повноваження доступу; авторизація.

Цілісність даних в блокчейн-системах (геш-функції).

Підписання даних (асиметрична криптографія).

Тема 10. Адреси та управління ключами. Типова структура транзакції. Смарт-контракти.

Адреси та управління ключами: формування адреси і поняття гаманця; створення, видалення, розповсюдження, зберігання ключів; генерація, знищення і заміна ключів; криптографічні алгоритми та довжини ключів.

Транзакції: типова структура; побудова; верифікація; питання конфіденційності даних і безпеки транзакцій.

Поняття смарт-контракту, приклади функціонування та застосування.

Тема 11. Типова структура блоку в блокчейн-ланцюгах. Види та побудова децентралізованих реєстрів.

Типова структура блоку у блокчейн-системах. Зв'язування блоків. Криптографічний одноразовий номер. Поняття та функції майнингу.

Децентралізовані реєстри: топологія структури реєстру; спрямований ациклічний граф.

Мітка часу. Методи децентралізованого узгодження часових інтервалів.

Тема 12. Розгалуження блокчейн реєстру.

М'які розгалуження (Soft Forks). Жорсткі розгалуження (Hard Forks). Конфлікти реєстру та їх вирішення. Поняття, створення та обробка застарілого (stale), сирітського (orphan) і спорідненого (uncle) блоку.

Тема 13. Моделі та механізми консенсусу.

Модель консенсусу з використанням механізмів: «Доказ виконаної роботи» (PoW); «Докази частки володіння» (PoS); Модель консенсусу на основі BFT-протоколів; Кругова модель консенсусу (Round Robin); Альтернативні механізми консенсусу засновані на доказах; Гібридні протоколи моделі консенсусу.

Поняття атаки подвійної витрати на алгоритми консенсусу з імовірнісною завершеністю. Аналіз провідних робот у даному напрямку. Визначення границі безпеки для протоколу PoW для мережі з затримкою доставки блоків та обчислення імовірності атаки подвійної витрати. Імовірність атаки подвійної витрати для протоколу PoS та знаходження кількості блоків підтвердження, для якої імовірність атаки є нехтувано малою.

Тема 14. Основні відомості про блокчейн біткоіна.

Загальні відомості про блокчейн біткоіна; Структура блоку біткоіна; Мережа біткоін – децентралізована мережева архітектура; Типи і ролі вузлів біткоін; Теоретичні відомості про біткоін і біткоін транзакції; Види транзакцій біткоіна; Структура транзакції біткоіна; Майнинг біткоіну.

Тема 15. Вимоги безпеки до пристроїв і платформ. Питання безпеки функціонування блокчейн систем.

Питання безпеки, що висувається до серверної та клієнтської частини, де функціонує програмне (апаратно-програмне) забезпечення блокчейн-системи. Можливість використання сервера для запуску інших застосунків.

Питання безпеки функціонування блокчейн-систем: інтерфейс API/протоколи, використовувані для відправки запиту; сумісність; структура даних, що зберігається; аудит; автентифікація вузла; життєвий цикл вузла; довгострокове управління даними блокчейна;

виправлення помилок у транзакціях; допоміжні/бічні ланцюги; ведення журналу подій; кібер і мережеві атаки.

Тема 16. Обмеження і омани, що пов'язані з технологією блокчейн.

Розглядаються наступні питання, пов'язані з функціонуванням блокчейн систем: незмінність; користувачі, які беруть участь в управління блокчейном; взаємодія з реальним світом; недобросовісні користувачі; відсутність довіри; використання ресурсів; невідповідні нагороди за публікацію в блоці; ідентичність цифрової особистості; продуктивність і масштабованість; проблема відповідальності.

3. Структура навчальної дисципліни

Назва розділів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		Л	ПЗ	Лаб.	Інд.	С.Р.
1	2	3	4	5	6	7
Тема 1. Феномен криптовалюти.	7	2	2			4
Тема 2. Криптовалюта та зловмисники.	7	2	2			3
Тема 3. ICO: що це і навіщо воно потрібно.	7	2	2			3
Тема 4. Інвестування у криптовалюти та кіберзлочинці.	7	2	2			3
Тема 5. Введення в технологію блокчейн і загальні поняття.	7	2	2			3
Тема 6. Блокчейн у світі.	7	2	2			3
Тема 7. Поняття подвійних витрат.	7	2	2			3
Тема 8. Протоколи на основі блокчейну. Смарт-контракти.	7	2	2			3
Тема 9. Огляд технології блокчейн. Основні механізми функціонування.	7	2	2			3
Тема 10. Адреси та управління ключами. Типова структура транзакції. Смарт-контракти.	7	2	2			3
Тема 11. Типова структура блоку в блокчейн-ланцюгах. Види та побудова децентралізованих реєстрів.	7	2	2			3
Тема 12. Розгалуження блокчейн реєстру.	7	2	2			3
Тема 13. Моделі та механізми консенсусу.	7	2	2			4
Тема 14. Основні відомості про блокчейн біткоіна.	7	2	2			3
Контрольна робота	8		2			6
Тема 15. Вимоги безпеки до пристроїв і платформ. Питання безпеки функціонування блокчейн систем.	7	2	1			3
Тема 16. Обмеження і омани, що пов'язані з технологією блокчейн.	7	2	1			3
Усього годин	120	32	32			56

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження хмарного майнинга та сервісів, що його надають.	2
2	Дослідження платформи Waves NG та її можливостей.	2
3	Дослідження поведінки курсу криптовалют на різних біржах.	2
4	Практичне застосування методики оцінювання проектів ICO.	2
5	Аналіз та дослідження існуючих криптовалют та механізмів їх роботи.	2
6	Аналіз та дослідження існуючих проектів на блокчейні та механізмів їх роботи.	2
7	Практичне дослідження існуючих смарт-контрактів.	2
8	Порівняння звичайних контрактів та смарт-контрактів.	2
9	Розгортання тестової блокчейн мережі.	4
10	Дослідження структури реєстру Біткоіна: взаємозв'язок блоків, знаходження та перевірка геш-значення в ланцюгах блокчейна.	4
11	Дослідження структури реєстру Біткоіна: побудова графіку часу на формування блоку.	4
12	Дослідження структури реєстру Біткоіна: перевірка древа Меркла у блоці, на підставі блокчейн-реєстру, побудова історичного графіку завантаження сеті біткоін.	4
	Разом	32

5. Завдання для самостійної роботи

№ з/п	Види та зміст завдання	Кількість годин
1	Підготовка до лекцій	**8**
1.1	Повторення основних положень технології блокчейн	2
1.2	Повторення поняття основних засад функціонування децентралізованих мереж	2
1.3	Повторення основних дій побудови блокчейн-реєстру	2
1.4	Повторення принципів у одноранговій мережевій взаємодії	2
2	Підготовка до практичних занять	**12**
2.1	Вивчення структури блокчейн-реєстру біткоіна	4
2.2	Визначення (створення) програмного забезпечення для взаємодії з блокчейн-реєстром	8
3	Підготовка доповіді та оформлення реферату за обраною темою	**20**
4	Підготовка до контрольної роботи	**6**
5	Вивчення додаткової літератури	**10**
	Разом	**56**

6. Індивідуальні завдання

Індивідуальне завдання – реферати за обраною студентом темою роботи стосовно технології блокчейн.

Суть завдання, що виконується за темою реферату, полягає у дослідженні можливостей, перспектив та загроз блокчейн систем, а також набуття практичних навичок з використання розподілених технологій блокчейну.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

8. Методи контролю

Контроль засвоєння студентами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

На практичному зайнятті або лекції контроль знань студентів робиться методом проведення експрес-опитувань (письмово). Максимальна кількість балів за продемонстровані студентами на експрес-опитуванні складає **24** бали.

На практичних роботах контроль засвоєння студентами навчального матеріалу здійснюється шляхом оцінки якості виконання завдання. Рівень знань, продемонстрований студентами при виконанні завдань оцінюється максимально **10** балами.

Контроль засвоєння студентами навчального матеріалу здійснюється на контрольній роботі, що передбачена навчальним планом. Рівень знань, продемонстрований студентами на контрольній роботі оцінюється максимально **10** балами.

При виконанні рефератів контролюється рівень засвоєння студентами системного розуміння проблеми. Бали за реферати складаються з розрахунку: 2,5 балів за зміст і акуратність, і 2,5 балів за захист роботи. Максимальна кількість балів за кожен реферат складає **5** балів. Передбачається виконання студентом двох рефератів.

Якість та повнота ведення конспекту лекційних та практичних занять оцінується до **6** балів включно.

Максимальна кількість балів за результатами контролю поточної успішності складає **60** балів.

Згідно рішення кафедри безпеки інформаційних систем і технологій до іспиту не допускаються студенти, що не брали участь у виконанні контрольних робіт і на протязі учбового курсу набрали менш 10 балів.

Підсумковий контроль здійснюється шляхом проведення іспиту.

Екзаменаційний квиток включає чотири теоретичних питання. Теоретичні питання оцінюються в залежності від складності та встановлюється для кожного питання окремо. Максимальна кількість балів за результатами іспиту складає 40 балів.

Максимальна кількість балів за результатами вивчення дисципліні складає 100 балів.

9. Схема нарахування балів

Бали за поточний контроль знань протягом семестру	Ведення конспекту лекції	Виконання практичних завдань	Контрольна робота, передбачена навчальним планом	Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
24	6	10	5	15	60	40	100

Критерії оцінювання

Критерії оцінювання знань студентів на експрес-опитування

Визначення	Кількість балів
Відповідь без помилок.	2
Виконання відповіді з незначними помилками.	1
Відповідь є з певною кількістю помилок, які не заважають достатньо повному висвітленню питання.	0,5
Неправильна відповідь, мають місце грубі помилки, нерозуміння суті питання.	0

Критерії оцінювання знань студентів за виконання практичної роботи

Визначення	Кількість балів
Завдання за практичною роботою виконане самостійно в повному обсязі. При захисті показано розуміння суті і змісту проведених досліджень.	5
Завдання за практичною роботою виконане самостійно в повному обсязі. При захисті результатів були виявлені незначні помилки у знанні теоретичного матеріалу.	4
Завдання за практичною роботою виконане в повному обсязі. При захисті результатів були виявлені незначні помилки у знанні теоретичного матеріалу.	2,5
Завдання за практичною роботою виконане. При захисті роботи були виявлені суттєві помилки у знанні теоретичного матеріалу.	1

Критерії оцінювання знань студентів за виконання контрольної роботи

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання, показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки.	10
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок, зроблені достатньо повні і правильні висновки.	5-9
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки.	2-4
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок у відповіді.	1
У відповідях показано слабкі знання навчального матеріалу.	0,5

Критерії оцінювання знань студентів за виконання рефератів

Визначення	Кількість балів
Завдання за обраними темами доповіді виконано акуратно та відповідає меті роботи. Студент показав тверде знання навчального матеріалу, вміння чітко і стисло викладати основні результати дослідження.	5
Завдання за темами доповіді виконано досить акуратно, але не у повній мірі відповідає поставленим питанням. Студент показав достатньо тверде знання навчального матеріалу і вміння стисло викладати основні результати дослідження.	4
Завдання за темами доповіді виконано не в повному обсязі. Студент показав не достатньо тверде знання навчального матеріалу і вміння викладати основні результати дослідження.	2-3
Завдання за темами доповіді виконано не в повному обсязі. Студент показав слабке знання навчального матеріалу і невміння викладати основні результати дослідження.	1

Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів
При відповіді на екзаменаційний білет теоретичні питання освітлені повністю.	40
При відповіді на екзаменаційний білет теоретичні питання достатньо освітлені, але з незначними помилками.	30-39
При відповіді на екзаменаційний білет теоретичні питання освітлені з значними помилками.	10-29
При відповіді на екзаменаційний білет теоретичні питання освітлені з суттєвими помилками або не надано правильних відповідей.	0-9

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирирівневої шкали оцінювання (іспит)
90-100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

10. Рекомендована література

Базова література

1. Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Режим доступу: https://bitcoin.org/bitcoin.pdf.
2. BitInfoCharts. Статистика криптовалюта. Режим доступу: https://bitinfocharts.com/.
3. NISTIR 8202 Blockchain Technology Overview. Режим доступу: https://doi.org/10.6028/NIST.IR.8202.
4. ASC X9 Study Group Report Distributed Ledger and Blockchain Technology Study Group. Режим доступу: https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf.
5. DIN SPEC 3104:2019-04. Blockchain-based validation of data. Режим доступу: https://dx.doi.org/10.31030/3042007.
6. Блокчейн и децентралізовані системи: навч. посібник для студ. закладів виш. освіти: в 3 частинах. Ч.1 / Кравченко П., Скрябин Б., Дубинина О. – Харків: ПРОМАРТ, 2018. 440с.

Допоміжна література

7. Блокчейн. Bitcoin Wiki. Режим доступа: https://ru.bitcoinwiki.org/wiki/Блокчейн.
8. Greenspan, G. “The Blockchain Immutability Myth.” CoinDesk, May 9, 2017. Режим доступу: https://www.coindesk.com/blockchain-immutability-myth/.
9. Обозреватель блоков. Режим доступа: https://www.blockchain.com/explorer.
10. Cedric Walter. Blockchain Consensus. Режим доступу: https://tokens-economy.gitbook.io/consensus/.
11. Криптовалюта: що це таке і які перспективи її поширення – думка експертів. Режим доступу: http://groshi-v-kredit.org.ua/kryptovalyuta-scho-tse-take-i-yaki-perspektyvy-jiji-poshyrennya-dumka-ekspertiv.html.
12. Криптовалюта: що це таке історія її створення. Режим доступу: https://pingblockchain.com/kriptovaljuta-shho-ce-take-istorija-ii-stvorennja/.
13. Що таке криптовалюта? Режим доступу: http://vidpovim.pp.ua/shho-take-kriptovalyuta/.
14. Цікаві факти про bitcoin. Режим доступу: https://cikavo-znaty.com/21-tsiikavyi-fakt-pro-bitcoin/.
15. Найпопулярніші криптовалюти. Режим доступу: https://ukr.media/criptovalyta/327316/.
16. Топ-10 найпопулярніших криптовалют у світі. Режим доступу: https://www.slovoidilo.ua/2018/02/05/infografika/finansy/top-10-najpopulyarnishyx-kryptovalyut-sviti.
17. Що таке майнінг, його значення для функціонування криптовалют. Режим доступу: http://coinews.io/ua/category/78-osnovi/article/630-shho-take-majn%D1%96ng,-jogo-znachennya-dlya-funkc%D1%96onuvannya-kriptovaljut.
18. Найпопулярніші криптовалюти світу. Окрім біткоіна. Режим доступу: https://espreso.tv/article/2017/08/30/alternatyvni_kryptovalyuta.
19. Що таке криптовалюта простими словами? Режим доступу: https://biznesua.com.ua/shho-take-kriptovalyuta-prostimi-slovami/.
20. Криптовалюта. Режим доступу: https://uk.wikipedia.org/wiki/Криптовалюта.
21. Київська митниця конфіскувала 200 ASIC-майнерів. Режим доступу: https://cryptobook.pro/kyyivs-ka-mytnytsya-konfiskuvala-200-asic-mayneriv.html.
22. Де і як майнити Ethereum за допомогою відеокарти. Режим доступу: https://cryptobook.pro/de-i-yak-maynyty-ethereum-za-dopomogoyu-videokarty.html.

23. Галушка Є.О., Пакон О.Д. Сутність криптовалют та перспективи їх розвитку // Молодий вчений. – № 4(44). – Квітень, 2017. – С. 634-638.
24. Оліярник М. Криптовалюта в Україні. Все, що потрібно знати // Новое время. Режим доступу: https://nv.ua/ukr/techno/it-industry/kriptovaljuta-bitcoin-v-ukrajini-vse-shcho-treba-znati-1918518.html.
25. https://forklog.com/ico-i-kraudsejl-yuridicheskij-likbez-dlya-kriptoinvestorov/.