

## СКОРОЧЕНИЙ ОПИС ДИСЦИПЛІНИ

### ЗАХИЩЕНІ ДЕЦЕНТРАЛІЗОВАНІ БЛОКЧЕЙН СИСТЕМИ

(назва дисципліни)

Обсяг дисципліни 4 кредити ЄКТС: лекцій 24 год., практичних занять 12 год., лабораторних занять 12 год., консультації 8 год., самостійна робота 64 год.

Форма контролю - Залік.

#### 1. Перелік тем дисципліни.

Змістовий модуль 1. Методи забезпечення безпеки даних в децентралізованих блокчейн системах.

Тема 1. Вступ в дисципліну. Технологія децентралізованих блокчейн систем.

Тема 2. Функціонування децентралізованих систем, які побудовані за технологією Blockchain.

Тема 3. Методи криптографії в децентралізованих блокчейн системах.

Тема 4. Різновиди цифрових підписів, які застосовуються в децентралізованих блокчейн системах.

Тема 5. Особливості застосування основних методів хешування в блокчейн системах.

Тема 6. Формати ключів та адрес. Особливості генерації ключів та адрес для блокчейн систем.

Змістовий модуль 2. Особливості функціонування децентралізованих блокчейн систем.

Тема 7. Побудова та взаємозв'язок даних в блокчейн системах. Концепція застосування дерева Меркла (Merkle tree).

Тема 8. Особливості функціонування відомих децентралізованих систем з блокчейн технологією (Ethereum, Monero, EOS).

Тема 9. Реалізація платіжних каналів як складова системи захисту даних.

Тема 10. Аналіз основних протоколів блокчейн систем. Формати транзакцій і блоків.

Тема 11. Методи забезпечення конфіденційності в блокчейн системах. Стандарти та підписи CryptoNote.

Тема 12. Методи підвищення конфіденційності в блокчейн системах. Протокол та модель транзакцій MimbleWimble.

#### 2. Вимоги до попередньо набутих компетентностей (за потребою).

- знання та розуміння предметної області та розуміння професії (КЗ 2);
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово (КЗ 3);
- здатність до пошуку, оброблення та аналізу інформації (КЗ 5).
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки (КФ 12).

3. Перелік компетентностей, яких набуде здобувач вищої освіти після опанування даної дисципліни.

- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки (КФ2);
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки (КФ 4);
- здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності (КФ 10);
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних(автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки (КФ 11).

4. Перелік результатів навчання, яких набуде здобувач вищої освіти після опанування даної дисципліни.

- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації (РН 1);
- 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 (РН 4);
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки (РН 9);
- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій (РН 15);
- використовувати програмні та апаратно програмні комплекси захисту інформаційних ресурсів (РН 18);
- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах (РН 19);
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки (РН 22);
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах (РН 27);
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації (РН 47).

5. Кафедра, що пропонує дисципліну Безпеки інформаційних технологій

6. Провідний викладач (П.І.Б., посада, науковий ступінь, наукове звання):

Власов Андрій Володимирович, доцент кафедри БІТ, кандидат технічних наук, старший дослідник