МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАНІКАЛО

BLOCKCHAIN: ОСНОВИ ТА ПРИКЛАДИ ЗАСТОСУВАННЯ
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 *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Долгова Н.Г., 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

Блокчейн – новітня технологія, інтерес до якої зріс разом з популярністю криптовалют. Але є десятки інших способів використання блокчейна у відриві від криптовалюти. Блокчейн-технологію відносять до головного технологічного прориву з часів винаходу Інтернету.

Предметом навчальної дисципліни вивчення навчальної дисципліни є теоретичні концепції, принципи функціонування та застосування блокчейн технологій.

Мета навчальної дисципліни – засвоєння теоретичних основ використання блокчейн технологій, основи криптовалют та смартконтрактів.

Результатом вивчення дисципліни є освоєння принципів застосування криптографічних методів у блокчейн технологіях; знання основних принципів криптовалют; основні обмеження та ризики створення та використання криптовалют; ознайомлення з методологічними основами розробки та функціонування блокчейн платформ..

Характеристика навчальної дисципліни

Курс	**3**
Семестр	**6**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Основи математичного моделювання	Комплексний курсовий проєкт
Основи криптографічного захисту	Основи стеганографічного захисту інформації
Інформаційні системи та інтернет-технології	Організаційне забезпечення захисту інформації
Безпека в інформаційно-комунікаційних системах	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
Здатність до пошуку, оброблення та аналізу інформації. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Розробляти моделі загроз та порушника;
Здатність до пошуку, оброблення та аналізу інформації. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	Аналізувати проекти інформаційно - телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно - телекомунікаційних системах програмно - апаратними засобами та давати оцінку результативності якості прийнятих рішень

інформаційної та/або кібербезпеки.	
Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	Використовувати сучасне програмно -апаратне забезпечення інформаційно - комунікаційних технологій
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
Знання та розуміння предметної області та розуміння професії. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	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;
Здатність застосовувати знання у практичних ситуаціях. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-	Використовувати програмні та програмноапаратні комплекси захисту інформаційних ресурсів

телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	
Здатність застосовувати знання у практичних ситуаціях. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно - телекомунікаційних системах
Здатність до пошуку, оброблення та аналізу інформації. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	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 системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або	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;

кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
Здатність застосовувати знання у практичних ситуаціях. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).	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;

Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	
Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
Знання та розуміння предметної області та розуміння професії. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. Здатність забезпечувати неперервність бізнесу згідно встановленої	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та

політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	Вирішувати задачі захисту інформації, що обробляється в інформаційно - телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	Забезпечувати) функціонування програмних та програмно - апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично - сигнатурних)
Здатність застосовувати знання у практичних ситуаціях. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1. ***Основи застосування криптографічних методів в блокчейн-технологіях***

Тема 1. *Технологія Блокчейн не тільки BitCoin*

Тема 2. *Принцип роботи BitCoin*

Тема 3. *Застосування криптографії в блокчейн*

Змістовий модуль 2. ***Основи блокчейн технологій та приклади застосування***

Тема 4. *Правила формування блоків в блокчейн.*

Тема 5. *Правила роботи блокчейн в біткойн*

Тема 6. *Проведення транзакцій та формати ключів в біткойн*

Тема 7. *Блокчейн та смарт-кантракти*

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, індивідуальні та групові міні-проекти.

Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу (теми 1-7), приклади застосування технології блокчейн (теми 1-7), з наданням пояснень у графічному вигляді (схеми, таблиці, презентації) та за допомогою прикладів конкретної реалізації сучасних проектів криптовалют (теми 1-7). На лабораторних заняттях здобувачі мають змогу отримати практичні навички пошуку вирішення проблем на підставі вихідних даних, сформульованих за тематикою заняття (теми 1-7). Вдосконалення практичних навичок відбувається під час виконання самостійної роботи (теми 1-7).

Наведені методи навчання спрямовані на формування у здобувачів здатності розв’язання складних комплексних задач використання технології блокчейн.

Порядок оцінювання результатів навчання

Програма навчальної дисципліни передбачає лекційні, лабораторні та самостійну види робіт. Знання та компетентності отримані здобувачами під час лекційних занять оцінюються за написання контрольних робіт та складання тестів, навички отримані під час лабораторних занять оцінюються за розв’язанням задач передбачених тематикою роботи. Самостійна робота окремо не оцінюється, оскільки вона полягає у підготовці до інших видів занять.

Розподіл балів поточного оцінювання за видами робіт є наступним.

Лабораторні заняття: рівень оволодіння теоретичними знаннями визначається під час захисту лабораторних робіт, за написання контрольних робіт та експрес-опитування. (максимальна кількість балів за написання контрольних робіт - 10 та експрес-опитування становить – 10). Рівень набутих навичок застосування знань для розв’язання задач визначається правильністю виконання завдань лабораторних робіт (максимальна кількість балів становить 40).

Самостійна робота: рівень оволодіння навичками використання новітніх знань, методології та методів проведення наукових досліджень визначається за ступенем підготовки аспіранта до виконання лабораторних робіт та написання контрольних робіт (в технологічній карті додаткових балів на цей вид робіт не передбачено).

Підсумковий контроль: проводиться з урахуванням екзамену.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування здобувачами компетентностей. Кожен екзаменаційний білет складається із 2 теоретичних питань та 1 практичного завдання, які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента та рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше теоретичне питання оцінюється 10 балами; друге питання оцінюється 10 балами; третє практичне завдання – розрахункове, виконання його оцінюється 20 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності". Здобувача слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або

перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та 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.

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

Рейтинг-план навчальної дисципліни

Теми	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Лекція *"Технологія Блокчейн не тільки BitCoin"*	Робота на лекції	
	Лабораторне заняття	*Лабораторна робота №1. Основи взаємодії з інтерфейсом Bitcoin вузла*		
	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 *"Принципи роботи біткойн"*	Робота на лекції	
	Лабораторне заняття	*Лабораторна робота №1. Основи взаємодії з інтерфейсом Bitcoin вузла*	Захист лабораторних робіт № 1	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 3	***Аудиторна робота***			
	Лекція	Лекція *"Застосування криптографії в блокчейн"*	Робота на лекції	
			експрес-опитування	5
	Лабораторне заняття	*Лабораторна робота №2. Робота з тестовою мережею Ethereum*	Захист лабораторних робіт № 2	8
			контрольна робота 1	5
	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 *"Правила формування блоків в блокчейн"*	Робота на лекції	
	Лабораторне заняття	*Лабораторна робота №3. Робота з тестовою мережею Monero*	Захист лабораторних робіт № 3	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 5	***Аудиторна робота***			
	Лекція	Лекція *"Правила роботи блокчейн в біткойн"*	Робота на лекції	
	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		
	Аудиторна робота			
Тема 6	Лекція	Лекція *"Проведення транзакцій та формати ключів в біткойн"*	Робота на лекції	
	Лабораторне заняття	*Лабораторна робота № 4. Основи взаємодії з інтерфейсами тестової мережі EOS*	Захист лабораторних робіт № 4	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		
	Аудиторна робота			
Тема 7	Лекція	Лекція *"Криптографія в біткойн"*	Робота на лекції	
			Експрес-опитування	5

	Лабораторне заняття	*Лабораторна робота № 5. Робота з децентралізованим сховищем даних IPFS*	Захист лабораторної роботи № 5	8
			контрольна робота 2	5
	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		
Екзамен				40
Загальна кількість балів				100

Рекомендована література

Основна

1. Кравченко П. Блокчейн і децентралізовані системи. Ч. 1 – Харків: ПРОМАРТ, 2019. – 452 с.
2. Кравченко П. Блокчейн і децентралізовані системи. Ч. 3 – Харків: ПРОМАРТ, 2020. – 306 с.

Додаткова

3. Могайар В. Блокчейн для бізнесу [Електронний ресурс] / Вільям Могайар // loveread.ec. 2018. Режим доступу до ресурсу: http://loveread.ec/read_book.php?id=71219&p=5.
4. Накамото С. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoci Накамото. URL: https://bitcoin.org/bitcoin.pdf
5. Бауэр В. П. Блокчейн как основа формирования дополненной реальности в цифровой экономике /В. П. Бауэр, С. Н. Сильвестров, П. Ю. Барышников // Информационное общество. – 2018. – № 3. – С. 30–40.
6. Розвиток блокчейн-бізнесу сприятимеекономічному відновленню України // http://www.fin.org.ua/news/1452566[Електронний ресурс].
7. UA Крипта в Україні 2021 —гравці, закони, тенденції. URL: https://nachasi.com/crypto/2021/05/31/cryptotrends-in-ukraine/[Електронний ресурс].

Інформаційні ресурси.

8. www.coindesk.com/information/applications-use-cases-blockchains/
9. https://www.nasdaq.com/article/4-innovative-use-cases-for-blockchain-cm901636
10. Starting 16 minutes: https://www.youtube.com/watch?v=cHe_ow9v094
11. https://blockchain.hneu.edu.ua/
12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною “Blockchain: основи та приклади застосування” https://pns.hneu.edu.ua/course/view.php?id=9664