МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Кафедра _____*кібербезпеки*_____
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність _____*125 Кібербезпека*_____
(шифр і назва)

освітня програма _____*Кібербезпека*_____
(назви освітньої програми)

вид дисципліни _____*спеціальна (фахова) підготовка; вибіркова*_____
(загальна підготовка /спеціальна (фахова) підготовка; обов’язкова/вибіркова)

форма навчання _____*денна*_____
(денна / заочна/дистанційна)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної исципліни
ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ
(назва дисципліни)

Розробники:

проф, д.т.н., проф.,		*Сергій ЄВСЕЄВ*
(посада, науковий ступінь та вчене звання)	(підпис)	(ім'я та прізвище)
доц.к.т.н.		*Наталя ВОРОПАЙ*
(посада, науковий ступінь та вчене звання)	(підпис)	(ім'я та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

кібербезпеки
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від "_22_" __серпня___2022 року № 1

Завідувач кафедри		*Сергій ЄВСЕЄВ*
	(підпис)	(ім'я та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми _____125 “Кібербезпека”_____

_____

Кафедра _____кібербезпеки_____
(назва кафедри на якій викладається дисципліна)

Гарант ОП  22.08.2022р *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

Завідувач кафедрою  22.08.2022р *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни "Децентралізовані системи" – засвоєння теоретичних основ та отримання практичних навичок використання децентралізованих технологій, принципів формування mesh networks.

Компетентності та результати навчання

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 системах; 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; РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23. реалізовувати заходи з протидії отриманню

Компетентності	Результати навчання
	несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 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); 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; 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; РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 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; 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; РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; 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; 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;

Компетентності	Результати навчання
	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 ріні 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–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; 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.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	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,

Компетентності	Результати навчання
	топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 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; 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; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; 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; 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 ріні класи політик

Компетентності	Результати навчання
	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.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	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–31застосовувати 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

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

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Комплексні системи захисту інформації	Безпека Інтернет-речей
Безпека в інформаційно-комунікаційних системах	Організація і безпека баз даних
Введення в мережі	Основи технічного захисту інформації
Основи математичного моделювання систем безпеки	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Всього (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
7	**90/3**	**48**	**42**	**32**	**16**	**–**	**–**	**2**	**–**	**+**

Співвідношення кількості годин аудиторних занять до загального обсягу складає 60 (%).

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	Л	2	**Тема 1. Децентралізація в інформаційних системах.** Поняття децентралізації для інформаційних систем. Децентралізовані файлообмінні системи. Застосування принципів децентралізації. Типова архітектура децентралізованих систем. Переваги та обмеження децентралізованих систем	1–3, 5–7
	СР	2		
2	Л	2	**Тема 2. Децентралізація як підхід в інформаційних системах.** Пірингові мережі та протокол BitTorren. Принципи побудови одноранговій файлообмінної мережі. Принцип роботи та застосування Distributed Hash Table. Концепція web-of-trust. Принципи функціонування web-of-trust, BitMessage, IPFS. Алгоритм досягнення консенсусу у Filecoin	1–3,5–7
	ЛЗ	2	**Лабораторне заняття № 1**. Реалізація “baby” blockchain. Діаграма класів. Клас Hash. Клас KeyPair. Клас Signature.	
	СР	2		
3	Л	2	**Тема 3. Криптографія у децентралізованих системах.** Генерація та обробка ключових даних. Принципи генерації ключів. Генератори випадкових послідовностей. Генератори псевдовипадкових послідовностей. Функції породження ключів (KDF). Протоколи обміну ключами. Протокол Діффі-Хеллмана на еліптичних кривих. Протокол EKE. Концепція та застосування Merkle Tree. Різновиди цифрових підписів. Lamport one time signature. Winternitz one time signature. Мультипідпис. Пороговий підпис. Груповий підпис. Кільцевий підпис. Сліпа підпис	1–4
	СР	2		
4	Л	2	**Тема 4. Bitcoin як платформа.** One-way peg and two-way peg sidechains. Пристрій Lightning Network. Механізм штрафування за шахрайство у каналі. Принципи роботи та застосування atomic swap. Застосування atomic swaps децентралізованими біржами. Proof-of-stake алгоритми досягнення консенсусу. Основні недоліки та ризики при	1–3

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
			використанні proof-of-stake.	
	ЛЗ СР	2 2	**Лабораторне заняття № 2**. Реалізація “baby” blockchain. Класс Account. Клас Operation. Клас Transaction.	1–4
5	Л СР	2 2	**<u>Тема 5.</u> Методи забезпечення конфіденційності у сучасних облікових системах.** Стандарти CryptoNote. Модель транзакцій MimbleWimble. Принципи гомоморфного шифрування. Quadratic Arithmetic Programs	1–3
6	Л	2	**<u>Тема 6.</u> Розвиток децентралізованих технологій.** Влаштування протоколу Bitshares. Decentralised asset exchange. SmartCoins. Організація бази даних. Оптимізація виконання бізнес-логіки.	1–3, 4
	ЛЗ СР	2 2	**Лабораторне заняття № 3**. Реалізація “baby” blockchain. Клас Block. Клас Blockchain	
7	Л СР	2 2	**<u>Тема 7.</u> Застосування децентралізованих підходів для організації різних систем.** Принципи функціонування та розвиток mesh network. Популярні протоколи для організації mesh-мереж. Децентралізовані системи цифрової ідентифікації. Протоколи OpenID та OpenID Connect. Розширення можливостей глобальної системи ідентифікації за допомогою технології blockchain.	1–3, 4
8	Л СР	2 2	**<u>Тема 8.</u> Децентралізовані платформи електронного голосування.** Децентралізований підхід до проведення електронного голосування. Використання технології blockchain для системи електронного голосування.	1–3
	ЛЗ СР	2 2	**Лабораторне заняття № 4. Реалізація криптографічного алгоритму.** Vigenère Cipher. Шифр AES.	1–3
9	Л СР	2 2	**<u>Тема 9.</u> Технології децентралізованих бірж.** Принципи функціонування децентралізованих бірж. Escrow. Atomic Swap. 0x Protocol. Internal exchanges.	1–3
10	Л СР	2 2	**<u>Тема 9.</u> Технології децентралізованих бірж.** Принципи функціонування децентралізованих бірж. Escrow. Atomic Swap. 0x Protocol. Internal exchanges.	1–3
	ЛЗ СР	2 2	**Лабораторне заняття № 4. Реалізація криптографічного алгоритму.** Vigenère Cipher. Шифр AES.	1–3

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
11	Л СР	2 2	**<u>Тема 10.</u> Децентралізований аукціон.** Принцип роботи онлайн-аукціону. Принцип роботи децентралізованого онлайн-аукціону	1–3, 4
12	Л СР	2 2	**<u>Тема 10.</u> Децентралізований аукціон.** Принцип роботи онлайн-аукціону. Принцип роботи децентралізованого онлайн-аукціону	1–3, 4
	Л СР	2 2	**Лабораторне заняття № 5. Реалізація криптографічного алгоритму.** SHA-1. Keccak	1–3
13	Л СР	2 2	**<u>Тема 11.</u> Використання концепцій sharding, off-chain і dag для масштабування облікових систем.** Використання off-chain протоколів. Sharding у blockchain-based системах. Обмін повідомленнями між shardchains. Конструкція та застосування Directed acyclic graph Архітектура розподілених облікових систем на основі DAG.	1–3
14	Л СР	2 2	**<u>Тема 11.</u> Використання концепцій sharding, off-chain і dag для масштабування облікових систем.** Використання off-chain протоколів. Sharding у blockchain-based системах. Обмін повідомленнями між shardchains. Конструкція та застосування Directed acyclic graph Архітектура розподілених облікових систем на основі DAG.	1–3
	ЛЗ СР	2 2	**Лабораторне заняття № 6. Реалізація криптографічного алгоритму.** RSA. ECDSA. Підписи Шнорра. Ring traceable signatures	1–3
15	Л СР	2 2	**<u>Тема 12.</u> Особливості і роль криптографічних зобов'язань в облікових системах**. Особливості та методи побудови криптографічних зобов’язань. Зобов’язання Педерсена. Підміна знань та підходи Nothing Up My Sleeve. Схема ElGamal commitment. Протокол ідентифікації Шнорра як інтерактивного схема докази з нульовим розголошенням. Схема ідентифікації Шнорра. Використання зобов’язань Педерсена для доказів із нульовим розголошенням. Використання зобов’язань Педерсена у Confidential Transaction. Алгоритми підпису, які будуються на використанні геш-функцій. Конструкція HORS. Схема підпису Меркла. Сімейство алгоритмів Sphincs.	1–3
16	Л	2	**<u>Тема 12.</u> Особливості і роль криптографічних зобов'язань в облікових системах**. Особливості та	1–3

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	СР	2	методи побудови криптографічних зобов'язань. Зобов'язання Педерсена. Підміна знань та підходи Nothing Up My Sleeve. Схема ElGamal commitment. Протокол ідентифікації Шнорра як інтерактивного схема докази з нульовим розголошенням. Схема ідентифікації Шнорра. Використання зобов'язань Педерсена для доказів із нульовим розголошенням. Використання зобов'язань Педерсена у Confidential Transaction. Алгоритми підпису, які будуються на використанні геш-функцій. Конструкція HORS. Схема підпису Меркла. Сімейство алгоритмів Sphincs	
	ЛЗ	2	**Лабораторне заняття № 6. Реалізація криптографічного алгоритму.** RSA. ECDSA. Підписи Шнорра. Ring traceable signatures	1–3
	СР	2		
Разом (годин)		**90**		

САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	26
2	Підготовка до лабораторних занять	16
	Разом	**42**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом.

МЕТОДИ НАВЧАННЯ

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 презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт, проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань;

Семестровий контроль проводиться у формі екзамену відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Семестровий контроль проводиться по екзаменаційних білетах в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається допущеним до семестрового екзамену з навчальної дисципліни за умови повного відпрацювання усіх лабораторних робіт, виконання контрольних робіт та тестових опитувань, що передбачено навчальною програмою з дисципліни.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для іспиту

Контрольні роботи	Лабораторні роботи	КП	РГЗ	Індивідуальні завдання	Тощо	Іспит	Сума
30	30	–	–	–	–	40	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проєкти, тощо),

що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки "відмінно", "добре", "задовільно" чи "незадовільно") та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
90-100	A	Відмінно	**- Глибоке знання** навчального матеріалу, що містяться в **основних і додаткових літературних джерелах;** **- вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; **- вміння** проводити **теоретичні розрахунки**; **- відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;** **- вміння вирішувати складні практичні задачі.**	Відповіді на запитання можуть містити **незначні неточності**
			- Глибокий рівень знань в обсязі	Відповіді на запитання

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
82-89	B	Добре	**обов'язкового матеріалу**, - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	містять **певні неточності;**
75-81	C	Добре	- **Міцні знання** матеріалу, що вивчається, та його **практичного застосування;** - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **практичні задачі.**	- невміння використовувати теоретичні знання для вирішення **складних практичних задач.**
64-74	Д	Задовільно	- Знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	Невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	E	Задовільно	- Знання **основних фундаментальних положень** - вміння вирішувати найпростіші **практичні задачі**.	Незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні положення при

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	**негативні**
				розвязанні **практичних задач**
35-59	FX (потрібне додаткове вивчення)	Незадовільно	**Додаткове вивчення** матеріалу може бути виконане **в терміни, що передбачені навчальним планом**.	Незнання **основних фундаменталь них положень** навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - невміння розв’язувати **прості практичні задачі.**
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна **відсутність знань** значної частини навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; -незнання основних фундаментальн их положень; - невміння орієнтуватися під час розв’язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для першого (бакалаврського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074 та введено в дію з 2018/2019 навчального року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни.

4. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ” [Електроннийресурс]. – Режим доступу: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Блокчейн и децентрализованные системы: учеб. пособие для студ. заведенный выше. образования: в 3 частях. Ч. 1 / П. Кравченко, Б. Скрябин, А. Дубинина. – Харьков, 2019. – 488 с.
2	Блокчейн та децентралізовані системи: навч. посібник для студ. закладів вищої. освіти: у 3 частинах. Ч. 2/П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. – Харків, 2019. – 402 с
3	Блокчейн и децентрализованные системы : учеб. пособие для студ. заведений высш. образования : в 3 частях. Ч. 3 / П. Кравченко, Б. Скрябин, А. Курбатов, О. Дубинина. – Харьков: 2020. – 305 с.
4	Ю. І. Когут Технології блокчейн та криптовалюта: ризики та кібербезпека. – Київ: 2022. – 316 с.

Допоміжна література

5	Dragoslav D Siljak, Decentralized Control of Complex Systems, 2012.
6	Arthur G.O. Mutambara. Decentralized Estimation and Control for Multisensor Systems, 2019.
7	Anuj Bhatia. Centralized vs Decentralized Air-conditioning Systems: Quick Book, 2015.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Buterin. A next-generation smart contract and decentralized application platform, 2014. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed June 2018.
2. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ” [Електроннийресурс]. – Режим доступу: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8