МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

РОБОЧА ПРОГРАМА

навчальної дисципліни "Розслідування кіберінцидентів, пов’язаних з віртуальними активами"
основних компонент
освітньої програми другого рівня вищої освіти

125 Кібербезпека (Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол №7 від 30.08.2023

СХВАЛЕНО
Вченою радою факультету №4
Протокол № 8 від 16.08.2023

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол №7 від 29.08.2023

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол № 19 від 15.08.2023)

Розробник: професор кафедри протидії кіберзлочинності факультету №4, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Опис навчальної дисципліни

Найменування показників	**Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 3	12 Інформаційні технології 125 Кібербезпека та захист інформації (Безпека інформаційних та комунікаційних систем) магістр	Навчальний курс 1 Семестр 1 Види підсумкового контролю: - екзамен.

Розподіл навчальної дисципліни за видами занять:	
денна форма навчання	заочна форма навчання
Лекції – 20 год; Практичні заняття – 20 год; Самостійна робота – 80 год; Індивідуальні завдання: Реферати (тощо) – 1	Лекції – 4 год; Практичні заняття – 6 год; Самостійна робота – 110 год; Індивідуальні завдання: Реферати (тощо) – 1

2. Мета та завдання навчальної дисципліни

Мета: формування знань та вмінь здійснювати розслідування кіберінцидентів, пов'язаних з віртуальними активами.

Завдання:

- ознайомлення із механізмами безпеки блокчейн технологій, використання криптовалют та криптотокенів;
- формування навичок розслідування кіберінцидентів, пов'язаних з віртуальними активами.

Міждисциплінарні зв'язки: спирається на Прикладну криптологію за програмою бакалавра.

Очікувані результати навчання:

знати: механізмами безпеки блокчейн технологій, використання криптовалют та криптотокенів.

вміти: здійснювати розслідування кіберінцидентів, пов'язаних з віртуальними активами.

На вивчення навчальної дисципліни відводиться 120 годин/4 кредитів ECTS.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки	
Фахові компетентності спеціальності (КФ)	КФ.7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому
	КФ.11	Здатність управляти системою попередження, розкриття та розслідування правопорушень, здійснених з використанням можливостей кіберсфери.

3. Програма навчальної дисципліни

Тема 1. Основні відомості про криптосистеми

Криптосистеми з приватним ключем. Криптосистеми з публічним ключем. Гешування. Цифрові підписи.

Тема 2. Технології функціонування платіжних криптовалютних систем

Децентралізація в інформаційних системах. Зв'язування блоків даних (блокчейн). Досягнення консенсусу. Принципи побудови актуальних децентралізованих криптовалют. Ключі, адреси і акаунти актуальних платіжних криптовалютних систем. Смарт-контракти.

Тема 3. Окремі аспекти розслідування кіберінцедентів, пов'язаних з віртуальними активами

Методи і засоби дослідження руху криптоактивів. Технології ускладнення аналізу походження криптоактивів. Пошук слідів використання криптоактивів на комп'ютерних пристроях. Технології вилучення криптоактивів.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контролю
	Всього	з них:			
		лекції	Практичні заняття	Самостійна робота	
Семестр №1					
Тема №1. Основні відомості про криптосистеми	18	4	2	12	екзамен
Тема №2. Технології функціонування платіжних криптовалютних систем	54	12	6	36	
Тема №3. Окремі аспекти розслідування кіберінцедентів, пов'язаних з віртуальними активами	48	4	12	32	
Всього за семестр №1	**120**	**20**	**20**	**80**	

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контролю
	Всього	з них:			
		лекції	Практичні заняття	Самостійна робота	
Семестр №1					
Тема №1. Основні відомості про криптосистеми	18	1	1	16	екзамен
Тема №2. Технології функціонування платіжних криптовалютних систем	54	2	1	51	
Тема №3. Окремі аспекти розслідування кіберінцедентів, пов'язаних з віртуальними активами	48	1	4	43	
Всього за семестр №1	**120**	**4**	**6**	**110**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Основні відомості про криптосистеми	
Відпрацювати лекції за темою. Закінчити виконання практичних занять. Скласти порівняльну таблицю алгоритмів ЕП	2-7, ресурси Internet
Тема №2. Технології функціонування платіжних криптовалютних систем	
Відпрацювати лекції за темою. Закінчити виконання практичних занять. Скласти порівняльну таблицю криптовалют.	2-7, ресурси Internet
Тема №3. Окремі аспекти розслідування кіберінцедентів, пов'язаних з віртуальними активами	
Відпрацювати лекції за темою. Закінчити виконання практичних занять. Скласти порівняльну таблицю засобів розслідування кіберінцедентів, пов'язаних з віртуальними активами.	2-7, ресурси Internet

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Огляд актуальних криптовалют.
2. Галузі використання блокчейн технологій.
3. Порівняльний аналіз принципів захисту систем від зловживання послугами Proof of work і Proof of stake.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких здобувачі вищої освіти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

Контроль проводиться по тестових завданнях на підсумковому контролі – заліку.

Контрольні питання

1. Що таке m-of-n signature?
2. Що таке здача в bitcoin?
3. Чи може бути модифікований актуальний вміст минулої історії трансакцій?
4. Чому повинен довіряти користувач?
5. Яка ймовірність знаходження блоку майнером, який контролює 30% обчислювальної потужності?
6. Чому дорівнює комісія?
7. Навіщо потрібен blockchain?
8. Яка мета у mining pool?
9. Яким буде час генерації блоків для одного ізольованого сегменту Інтернет, якщо в ньому буде зосереджено ≈ 33% потужності, а в іншій частині Інтернету ≈ 66% обчислювальної потужності (до зміни складності)?
10. Чим обмінюються вузли мережі bitcoin?
11. Як голосувати проти трансакцій?
12. Як виглядають монети Bitcoin?
13. Чим визначається власник монети (НЕ витраченого виходу)?
14. Яке твердження для 2-of-3 і 2-of-2 multisignature схем авторизації у bitcoin є ПРАВИЛЬНИМ?
15. Що буде з мережею Bitcoin, коли після відсутності Інтернет з'явиться знову?
16. Навіщо в системі з'являються нові монети?
17. Хто може бачити баланс адреси?
18. Чому першим знаходити рішення задачі буде не завжди той, у кого найшвидший комп'ютер?
19. Як залежить ймовірність першим знайти блок від обчислювальної потужності?
20. Як одержувачу захиститися від double-spending?
21. Де зберігається баланс кожного облікового запису в bitcoin?
22. Як будуть заробляти майнери коли перестануть з’являтися нові bitcoin?
23. Який шанс вгадати з 1 разу 1 число зі 100?
24. Як ви думаєте, який обсяг даних приблизно займає весь блокчейн зараз?
25. Скільки мінімально відсотків обчислювальної потужності потрібно, щоб протягом тривалого часу перемагати частіше за інших?
26. Хто регулює систему bitcoin?
27. Як блоки зв'язні один з одним?
28. Що таке Smart-Contract?
29. У чому суть функції гешування?
30. Які архітектурні принципи використовуються в криптовалюті?
31. Які недоліки у протоколі bitcoin?
32. Хто може сформувати транзакцію, в якій Аліса платить Бобу?

33. Чи буде завдання майнерів однаковим, якщо вони голосують за однаковий набір трансакцій?
34. Як можна зберігати монети Bitcoin?
35. Як ви думаєте, як формується ціна на bitcoin?
36. Що таке nLockTime?
37. Які можуть бути use-cases множинних підписів?
38. Як знищити bitcoin мережу?
39. Скільки грошей витрачається з output попередньої транзакції?
40. Що таке fork?
41. Що таке proof-of-work?
42. Що буде з блокчейном якщо Інтернет між континентами пропаде?
43. Яку можливість дає multisig адреса?
44. Що потрібно для отримання і відправки платежів через протокол Bitcoin?
45. Де зберігається блокчейн?
46. Якщо перший учасник перебирає числа зі швидкістю 1 за секунду, а другий - 9 за секунду, то який шанс першим вгадати число у кожного із них?
47. Що потрібно знати для генерації нової адреси?
48. Від чого залежить винагорода майнерам?
49. Чому дорівнює приріст bitcoin в кожному блоці (2020 рік)?
50. Як вступають в силу оновлення протоколу bitcoin?
51. Що означає децентралізованість технології блокчейну?
52. Що таке майнінг криптовалюти?
53. Майнери об'єднуються у «пули». Навіщо вони це роблять?
54. Якщо хтось контролює більше половини всіх майнерів у світі, що він може зробити?
55. Що таке смарт-контракти?
56. Що, з точки зору анонімності, дає прийом пожертвувань в біткоїнах?
57. Чому в блокчейні біткоїну блок з трансакціями створюється приблизно один раз за 10 хвилин?
58. Що станеться, якщо кількість майнерів подвоїться?

Контрольні завдання

1. Яким був баланс BTC за адресою xxxx станом на xxxx?
2. Скільки BTC було надіслано за адресою xxxx у трансакції xxxx?
3. Скільки BTC склала комісія у трансакції xxxx?
4. Який розмір в байтах трансакції xxxx?
5. В який блок була включена трансакція xxxx?
6. Скільки BTC склала комісія за підтвердження блока xxxx?
7. Скільки трансакцій містить блок з гешом xxxx?
8. Скільки BTC було надіслано в блоці трансакцій за номером xxxx?
9. Яким є значення випадкового числа, за допомогою якого було знайдений геш блоку трансакцій за номером xxxx?
10. З якої адреси було надіслано xxxx BTC на адресу xxxx?

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\textit{Загальна кількість балів (перед підсумковим контролем)} = (\textit{Результат навчальних занять за семестр} + \textit{Результат самостійної роботи за семестр}) / 2 * 10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.***

Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни = ***Загальна кількість балів (перед підсумковим контролем)*** + ***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

Підсумкові бали навчальної дисципліни = ***Підсумкові бали за поточний семестр*** + ***Підсумкові бали за попередній семестр*** : ***2***

Критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97–100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85– 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
80-84			
75–79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
65-69			
60–64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
41–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки
21-40			
1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
			курсу **не призведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

1. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.
2. Кравченко П. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
3. Кравченко П. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 3 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2020. –305 с.
4. Носов В.В., Манжай І.А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. Право і безпека – Право и безопасность – Law and Safety. 2021. № 1 (80). с 93 – 100. DOI: https://doi.org/10.32631/pb.2021.1.13.
5. Носов, В. В., Манжай, О. В. і Панченко, Є. В. (2022) «Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень», Право і безпека, 87(4), с. 108-124. doi: 10.32631/pb.2022.4.09.

Додаткова

6. Blockchain and decentralized systems : in three volumes. V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kharkiv : PROMART, 2020. – 288 p.
7. Andreas M. Antonopoulos Mastering Bitcoin: Programming the Open Blockchain. Second edition: O'Reilly Media, 2017. - 405 p.
8. Manav Gupta. Blockchain For Dummies®, IBM Limited Edition: John Wiley&Sons, 2017.- 51 p.
9. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf.

Інформаційні ресурси

1. https://academy.binance.com/uk
2. https://ethereum.org/uk/developers/docs/
3. https://explorer.crystalblockchain.com/
4. https://intelx.io/tools?tab=bitcoin
5. https://www.breadcrumbs.app/home
6. https://etherscan.io/
7. https://www.walletexplorer.com/
8. https://www.aware-online.com/en/osint-tools/cryptocurrency-tools/