



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ

Факультет № 4
Кафедра протидії кіберзлочинності

ЗАТВЕРДЖЕНО

На спільному засіданні кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
протокол № 3 від 23.06.2023

Завідувач кафедри

Олександр МАНЖАЙ

**РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ, ПОВ'ЯЗАНИХ З
ВІРТУАЛЬНИМИ АКТИВАМИ (ОК.03)**

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	Носов Віталій Вікторович , професор кафедри протидії кіберзлочинності факультету № 4, кандидат технічних наук, доцент E-mail: vitnos@univd.edu.ua Лекційний потік: факультет № 4, шифр навчальних груп Ф5-104м
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Другий (магістерський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології

Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається у 1 семестрі I курсу навчання
Мета вивчення дисципліни	формування знань та вмінь здійснювати розслідування кіберінцидентів, пов'язаних з віртуальними активами
Завдання вивчення дисципліни	<ul style="list-style-type: none"> - ознайомлення із механізмами безпеки блокчейн технологій, використання криптовалют та криптокотенів; - формування навичок розслідування кіберінцидентів, пов'язаних з віртуальними активами.
Обсяг дисципліни в кредитах ECTS/годинах	Кількість кредитів ECTS - 4 (загальний обсяг – 120 год.)
	З них (денна/заочна):
	- аудиторна робота: 40/10 год. - самостійна робота: 80/110 год.
Форми та види проведення навчальних занять	Форма навчання – денна/заочна Види навчальних занять: - лекції: 20/4 год.; - практичні заняття: 20/6 год.
Самостійна робота	Опрацювання рекомендованої літератури, виконання домашніх завдань до практичних занять, виконання індивідуальних завдань до практичних занять
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до практичних занять
Необхідне обладнання	Мультимедійне обладнання (ноутбук, проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Методи контролю: поточний та підсумковий контроль (екзамен) Форми контролю: захист індивідуальних завдань на практичних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням.
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або

	кібербезпеки
Фахові компетентності (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.
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
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 кіберінцидентів, 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.	
Програмні результати навчання (РН)	РН.2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах
	РН.3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
	РН.5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення
	РН.6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

	технології створення та використання спеціалізованого програмного забезпечення
	РН.12. 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
	РН.16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень
	РН.19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності
	РН.20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик
	РН.21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки
	РН.22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
	РН.23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та

	довідкової літератури та іншої доступної інформації.
	РН.24. Здійснювати управління системою попередження, розкриття та розслідування правопорушень, вчинених з використанням можливостей кіберсфери.
Критерії оцінювання результатів навчання	<p>Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:</p> <ul style="list-style-type: none"> ● поточний контроль - 50 балів; ● підсумковий контроль - 50 балів. <p>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менше 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: захист звітів лабораторних робіт з коефіцієнтом 5.</p> <p>Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамен).</p>

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно («зараховано»)	А	«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»)	В	« 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		С	« 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»)	Д	« 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		Е	« 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
40 – 59	Незадовільно («не зараховано»)	Ф Х	« 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		Ф	« 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 курсу не призведе до значного підвищення якості виконання навчальних завдань, робота, що потребує повної переробки
Перелік питань, що виносяться на підсумковий контроль		
<ol style="list-style-type: none"> 1. Криптосистеми з приватним ключем. 2. Криптосистеми з публічним ключем. 3. Гешування. 4. Цифрові підписи. 5. Чисельне представлення інформації. 6. Децентралізація в інформаційних системах. 7. Архітектура і властивості зв'язаних блоків даних (блокчейн). 8. Механізми і протоколи досягнення консенсусу. 9. Принципи побудови актуальних децентралізованих криптовалют. 10. Ключі, адреси і акаунти актуальних платіжних криптовалютних систем. 11. Смарт-контракти. 12. Методи і засоби дослідження руху криптоактивів. 13. Мікшування криптоактивів. 14. Атомарний обмін криптоактивів. 15. Методи і засоби пошуку слідів використання криптоактивів на комп'ютерних пристроях. 16. Технології вилучення криптоактивів. 		
ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ Навчальна та наукова література <ol style="list-style-type: none"> 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 транзакцій 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-транзакцій під час попередження та розслідування кримінальних правопорушень», <i>Право і безпека</i>, 87(4), с. 108-124. doi: 10.32631/pb.2022.4.09. 		
ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ		

Навчальна та наукова література

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

Інформаційні ресурси в Інтернеті

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/>