

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра системного аналізу та інформаційних технологій

ЗАТВЕРДЖЕНО
протокол засідання кафедри
«28» серпня 2023 року № 1

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОКПІ 1.2.21. Теорія і практика інфраструктури відкритих
ключів
(шифр і назва навчальної дисципліни)

спеціальність 125 Кібербезпека
(шифр і назва спеціальності)

спеціалізація _
(назва спеціалізації)

факультет _____ економіко-правовий _____
(назва факультету)

2023-2024 рік

Робоча програма

Теорія і практика інфраструктури відкритих ключів для здобувачів вищої освіти ОП
125 Кібербезпека

(назва навчальної дисципліни)

першого (бакалаврського) рівня вищої освіти

Спеціальність 125 Кібербезпека

Розробники:

Неласа А.В., доцент кафедри САІТ, кандидат технічних наук, доцент

(вказати авторів, їхні посади, наукові ступені та вчені звання)

© Неласа А.В. 2023 р.

© МДУ, 2023 р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів –4	Галузь знань <u>12 Інформаційні технології</u> (шифр і назва)	Нормативна	
Модулів – 2	ОП <u>125 Кібербезпека</u> (шифр і назва) Спеціальність <u>Кібербезпека</u>	Рік підготовки:	
Змістових модулів –3		4-й	4-й
		Семестр	
Загальна кількість годин - 120		8-й	8-й
Тижневих годин для денної форми навчання: аудиторних - 4 самостійної роботи студента – 8	Рівень вищої освіти: бакалавр	Лекції	
		20 год.	6 год.
		Практичні, семінарські	
		Лабораторні	
		20 год	4 год.
		Самостійна робота	
		80 год.	110год.
		Індивідуальні завдання	
Вид контролю			
залік			

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання 50 %,

для заочної форми навчання 10%.

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни: закладання термінологічного фундаменту, навчання студентів основам сертифікації відкритих ключів, сучасним принципам побудови та застосування інфраструктури відкритих ключів, нормативному регулюванню та стандартизації ІВК.

Завдання навчальної дисципліни: У цьому курсі передбачається формування у студентів певних знань та вмінь з теорії та практики технології організації інфраструктури відкритих ключів.

Місце навчальної дисципліни в освітній програмі: ОК30. ОКПП 1.2.21.

Передумови для вивчення дисципліни: "Основи кібербезпеки", "Програмування", "Криптологія", "Нормативно-правове забезпечення інформаційної безпеки", "Комп'ютерні мережі", "Архітектура комп'ютерних систем", "Захист інформації в комп'ютерних системах та мережах".

Компетентності та результати навчання:

ПК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КФ 1. 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.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

РН2 організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН4 аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН11 виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

РН19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН21 вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно-телекомунікаційних (автоматизованих) системах;

РН22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки;

РН24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

РН26 впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

РН27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

РН31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН35 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;

РН46 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;

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи сертифікації відкритих ключів.

Тема 1. Вступ до інфраструктури відкритих ключів та системи ЕЦП.

Тема 2. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів.

Тема 3. Життєві цикли особистих ключів та сертифікатів відкритих ключів. Формат(и) особистих ключів.

Тема 4. Обслуговування сертифікатів відкритих ключів.

Змістовий модуль 2. Теоретичні основи побудови інфраструктури відкритих ключів.

Тема 5. Моделі та механізми електронних довірчих послуг. Електронні довірчі послуги на основі ЕЦП та НШ.

Тема 6. Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації

Тема 7. Валідація (перевірка) шляхів сертифікації при наданні електронних довірчих послуг.

Змістовий модуль 3. Нормативне регулювання та стандартизація інфраструктури відкритих ключів.

Тема 8. Стандартизація у галузі ІВК та надання електронних довірчих послуг.

Тема 9. Класифікація протоколів ІВК, особливості, застосування та аналіз.

Тема 10. Основні існуючі та перспективні положення політик сертифікації.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин										
	Денна форма						Заочна форма				
	Усього	у тому числі					Усього	у тому числі			
		л	п	лаб	сем	кон		с.р	л	п	лаб
Модуль 1											
Змістовий модуль 1. Основи сертифікації відкритих ключів											
Тема 1. Вступ до ІВК та національної системи ЕЦП		2		2			8				10
Тема 2. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів		2		2			8		1	2	10
Тема 3. Життєві цикли особистих ключів та сертифікатів відкритих ключів. Формат(и) особистих ключів		2		2			8		1		10
Тема 4. Обслуговування сертифікатів відкритих ключів. Аналіз та оцінка механізмів відкликання сертифікатів відкритих ключів		4		2			8				15
Разом за змістовим модулем 1		10		8			32		2	2	45
Усього годин за 1 модуль		10		8			32		2	2	45
Модуль 2											
Змістовий модуль 2. Теоретичні основи побудови інфраструктури відкритих ключів											
Тема 5. Моделі та механізми електронних довірчих послуг. Електронні довірчі послуги на основі ЕЦП та НШ	2		2		8			1		2	10
Тема 6. Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації	2		2		8			1			10
Тема 7. Валідація шляхів сертифікації при наданні електронних довірчих послуг	1		2		8						10
Разом за змістовим модулем 2	5		6		24			2		2	30

Змістовий модуль 3. Нормативне регулювання та стандартизація інфраструктури відкритих ключів											
Тема 8. Стандартизація у галузі ІВК та надання електронних довірчих послуг		2		2			8		1		15
Тема 9. Класифікація протоколів ІВК, особливості, застосування та аналіз		2		2			8		1		10
Тема 10. Основні існуючі та перспективні положення політик сертифікації. Проблеми теорії та практики надання електронних довірчих послуг		1		2			8				10
Разом за змістовим модулем 3		5		6			24		2		35
Усього годин за 2 модуль		10		12			48		4	2	65
Усього годин		20		20			80		6	4	110

5. Теми лабораторних занять

№ з/п	Назвтеми	Кількість годин	
1	Використання симетричних алгоритмів шифрування	4	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46, PH 48
2	Використання асиметричних алгоритмів шифрування	4	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46, PH 48
3	Використання електронного цифрового підпису	4	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46, PH 48
4	Створення і розподіл криптографічних ключів	4	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46 , PH 48
5	Створення сертифікатів відкритих ключів	4	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46, PH 48
	Усього	20	

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Національна та міжнародна нормативно – правова бази в частині ІВК (ЕЦП). Призначення та застосування національної системи ЕЦП	8
2	Базові архітектури ІВК, побудова шляхів сертифікації ключів та їх аналіз	8
3	Принципи побудування та функціонування національної системи ЕЦП. Центри сертифікації, вимоги до них та застосування	8
4	Механізми генерування асиметричних пар ключів на робочих станціях та на відокремлених пунктах реєстрації. Принципи реалізації ІВК	8
5	Сертифікати відкритих ключів. Прикладні формати сертифікатів та технічні специфікації для ІВК	8
6	Механізми виготовлення та обслуговування сертифікатів відкритих ключів в центрах сертифікації ключів	8
7	Шляхи сертифікації в системі ІВК (ЕЦП). Особливості застосування при наданні електронних довірчих послуг	8
8	Стандартизація у галузі ІВК. Нормативні та нормативно-технічні документи з регулювання діяльності ЦСК (АЦСК)	8
9	Криптографічні протоколи для надання в системі ЕЦП (ІВК) послуг цілісності, неспростовності, доступності та неспростовності	8
10	Проблеми теорії та практики удосконалення та розвитку систем и ІВК (ЕЦП). Перспективні політики сертифікації. Основні додатки застосування системи ЕЦП (ІВК) та оцінка їх ефективності.	8
Разом:		80

7. Методи навчання

Як форми контролю якості одержаних знань застосовуються :

- *вхідний контроль* знань з криптології та інформаційних технологій на початку вивчення дисципліни;
- *поточний рейтинговий контроль* за допомогою контрольних завдань, тестів та навчаючих програм безпосередньо на комп'ютері;
- *опит* під час захисту звітів з практичних робіт безпосередньо на комп'ютері;
- *контроль остаточних знань* під час завершення вивчення дисципліни.

За результатами контролю якості навчання студенти отримують *бали рейтингу*, які є підґрунтям для остаточної оцінки.

8. Засоби діагностики результатів навчання

Діагностика результатів навчання відбувається у формі поточного модульного контролю (тестування за змістовими модулями, усне опитування, захист лабораторних робіт, експрес-контроль), підсумкового контролю – у формі заліку.

9. Критерії оцінювання

Критерії поточного оцінювання знань студентів.

Усний виступ та виконання письмового завдання, тестування	Критерії оцінювання
5	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
4	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
3	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
2	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
1	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.

Доповнення виступу:

2 бали – отримують студенти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують студенти, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

Суттєві запитання до доповідачів:

2 бали отримують студенти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують студенти, які у своєму запитанні до виступаючого вимагають додаткової інформації з ключових проблем теми, що розглядається.

Експрес-контроль:

2 бали нараховуються студентам, які вільно володіють усім навчальним матеріалом, орієнтуються в темі та аргументовано висловлюють свої думки.

1 бал отримують студенти, які частково володіють матеріалом та можуть окреслити лише деякі проблеми теми.

Складання словника основних термінів, що визначені програмою курсу (за темами):

Програмою курсу визначено перелік ключових термінів, що розкривають зміст кожної теми. Студентам пропонується скласти словник основних термінів з конкретної теми на останніх сторінках опорного конспекту лекцій.

2 бали нараховуються студентам, які не лише склали повний перелік визначених термінів з конкретної теми, а й можуть вільно розтлумачити їх зміст.

1 бал нараховуються студентам, які склали неповний перелік визначених термінів з конкретної теми

і не можуть їх розтлумачити без конспекту.

Ведення опорного конспекту лекції:

2 бали нараховуються студентам, які в повному обсязі самостійно і творчо опрацювали всі питання лекції і вільно володіють її змістом.

1 бал нараховується студентам, які опрацювали лише окремі питання лекції і не достатньо вільно володіють її змістом.

Підготовка творчих завдань(есе, дайджест):

2 бали отримують студенти, які можуть виокремити з різних джерел основні положення, структурно об'єднати їх, коротко проаналізувати кожне з них та зробити ґрунтовні узагальнюючі висновки.

1 бал отримують студенти, які в цілому правильно виокремили основні положення кожного з джерел, але не зробили їх відповідного аналізу та узагальнюючих висновків.

Ведення конспекту першоджерел.

2 бали отримують студенти, які опрацювали всю необхідну обов'язкову літературу, засвоїли її основні теоретичні положення, вміють їх пояснити і розтлумачити.

1 бал отримують студенти, котрі опрацювали не всю необхідну літературу, не завжди розуміють її вихідні теоретичні положення, поверхово їх пояснюють.

Підсумковий модульний контроль знань студентів.

Критерії підсумкового модульного оцінювання знань студентів

Письмова контрольна робота або тестування	Критерії оцінювання
21-25	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
17-21	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
14-17	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
10-14	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
10	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

10. Розподіл балів, які отримують студенти

Вид роботи	Кількість годин	Обсяг кредитів	Кількість балів
Змістовий модуль 1. Математичні методи та симетричні криптографічні перетворення			
Тема 1. Вступ до інфраструктури відкритих ключів та системи ЕЦП.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 2. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 3. Життєві цикли особистих ключів та сертифікатів відкритих ключів. Формат(и) особистих ключів.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 4. Обслуговування сертифікатів відкритих ключів.			
лекційні	4	0,2	4
лабораторні заняття	2	0,2	4
Змістовий модуль 2. Теоретичні основи побудови інфраструктури відкритих ключів.			
Тема 5. Моделі та механізми електронних довірчих послуг. Електронні довірчі послуги на основі ЕЦП та НШ.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 6. Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 7. Валідація (перевірка) шляхів сертифікації при наданні електронних довірчих послуг.			
лекційні	1	0,2	4
лабораторні заняття	2	0,2	4
Змістовий модуль 3. Нормативне регулювання та стандартизація ІВК.			
Тема 8. Стандартизація у галузі ІВК та надання електронних довірчих послуг.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 9. Класифікація протоколів ІВК, особливості, застосування та аналіз.			
лекційні	2	0,2	4
лабораторні заняття	2	0,2	4
Тема 10. Основні існуючі та перспективні положення політик сертифікації.			
лекційні	1	0,2	4
лабораторні заняття	2	0,2	4
Тези/наук. стаття			20
Підсумок			100

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

12. Інструменти, обладнання та програмне забезпечення:

Під час викладання дисципліни для занять використовується лабораторна база комп'ютерних класів МДУ, які обладнано мережею комп'ютерів IBM Pentium та виходом до Інтернет.

Перелік програмного забезпечення: OpenSSL, Visual Studio.

13. Рекомендовані джерела інформації:

Обов'язкова література:

1. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX
2. Закон України «Про електронні довірчі послуги (Відомості Верховної Ради (ВВР), 2017, № 45, ст.400) <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
3. Закон України «Про електронні документи та електронний документообіг» (Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275) <https://zakon.rada.gov.ua/laws/show/851-15#Text>
4. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».
5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
6. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / [О. В. Потій, А. В. Леншин, Л. С. Сорока, В. І. Єсін і ін.]. – Дніпропетровськ: Академія митної служби України, 2011. – 202с.
7. Потій О.В., Іщенко Ю.М., Леншин А.В. Текст лекцій з дисципліни «Побудова та розгортання інфраструктури відкритих ключів», Харків, ХНУРЕ, 2009 р.
8. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.

Додаткова:

- .. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти управління ключами / О.В. Потій. – Х. : ХНУРЕ, 2002. – 80 с.
10. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти механізмів безпеки/ О.В. Потій. – Х. : ХНУРЕ, 2001. – 80 с.

11. Постанова Кабінету Міністрів України від 28.10.04.№1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади».
12. ITU-T Recommendation X.509. Information Technology - Open Systems Interconnection - The Directory Public Key and Attribute Certificate Frameworks. June 2000 (документ еквівалентен ISO/IEC 9594-8 Directory Services, 2000).

14. Політика навчальної дисципліни

Політика навчальної дисципліни «Теорія і практика інфраструктури відкритих ключів» заснована на положеннях Етичного кодексу, [Положенні про організацію контролю та оцінювання успішності навчання здобувачів вищої освіти](#), [Положенні про комплекс навчально-методичного забезпечення навчальної дисципліни](#), [Положенні про академічну доброчесність](#), [Положенні щодо політики розвитку soft skills](#) в Маріупольському державному університеті.

Вивчення дисципліни потребує підготовки до лекційних та лабораторних занять, виконання науково-дослідного завдання (реферативне дослідження, участь у конференції з публікацією тез або наукової статті), опрацювання рекомендованої основної та додаткової літератури.

Підготовка та виконання практичних робіт передбачає: ознайомлення з програмою навчальної дисципліни та планами практичних занять; вивчення теоретичного матеріалу; виконання завдань, запропонованих для самостійного опрацювання.

Відповідь здобувача повинна демонструвати ознаки самостійності виконання поставлених завдань, відсутність ознак повторюваності та плагіату. Присутність здобувачів вищої освіти на заняттях є обов'язковою. Пропущені з поважних причин заняття мають бути відпрацьовані.

Здобувач вищої освіти повинен дотримувати навчально-академічної етики та графіка навчального процесу.

15. Загальна інформація про навчальну дисципліну



Назва навчальної дисципліни	Теорія і практика інфраструктури відкритих ключів
Освітня програма	125 Кібербезпека
Рівень вищої освіти	перший (бакалавський)
Кафедра, яка здійснює викладання	Системного аналізу та інформаційних технологій
Викладач ШБ, посада	Неласа Г.В., доцент
Електронна адреса викладача	annanelasa@gmail.com
Консультації (дата, час, можливості он-лайн консультування)	Що середи 14.00-15.00
Посилання на сторінку навчальної дисципліни на Навчальному порталі МДУ	https://moodle.mu.edu.ua/enrol/index.php?id=12139
Компетентності та програмні результати навчання	PH2, PH4, PH11, PH19, PH21, PH22, PH24, PH26, PH27, PH31, PH35, PH46, PH48, ІК, К31, КФ 2, КФ 4, КФ 8.

Семестр вивчення	Обсяг (годин/кредити)	Кількість аудиторних годин			Кількість, види індивідуальних завдань	Форма контролю
		лек	лаб	Пр.		
5	150/5	26	16	18	Підготовка тез доповіді на конференції/статті, реферативне дослідження з обраної теми.	Залік

Завідувач кафедри

Ganna

Ганна МАРТИНЮК

Гарант ОП

Ganna

Ганна МАРТИНЮК