МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра математичних методів та системного аналізу

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.19. Теорія і практика інфраструктури відкритих ключів
(шифр і назва навчальної дисципліни)

Освітньо-професійна програма Кібербезпека
(назва)

Спеціальність 125 Кібербезпека
(код та найменування спеціальності)

Спеціалізація _____
(назва спеціалізації)

Факультет Економіко-правовий
(назва факультету)

2020 – 2021 рік

Робоча програма з дисципліни

Теорія і практика інфраструктури відкритих ключів

(назва навчальної дисципліни)

для студентів ОП Кібербезпека

за спеціальністю (напрямом підготовки) 125 Кібербезпека

Розробники:

Неласа Г.В. доцент кафедри математичних методів та системного аналізу аналізу

Морозова А.О. асистент кафедри математичних методів та системного аналізу аналізу

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

Робоча програма затверджена на засіданні

кафедри математичних методів та системного аналізу

Протокол від « 27 » серпня 2020 року, № 1

Завідувач кафедри

математичних методів та системного аналізу

(Т.В. Шабельник)

(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td>Галузь знань:
12 Інформаційні технології
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">ОП
Кібербезпека
(назва)
Спеціальність
125 Кібербезпека
(код та найменування спеціальності)</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>4-й</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання
вирішення типових завдань за темами змістових модулів</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин - 150</td><td>8-й</td><td>8-й</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання: аудиторних -4 самостійної роботи студента – 8</td><td rowspan="11">Освітній рівень:
магістр</td><td colspan="2">Лекції</td></tr>
<tr><td>26 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>10 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>98 год.</td><td>128 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2">2 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Примітка.

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

для денної форми навчання 33,3 %,

для заочної форми навчання 13,3 %

2. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни: навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення безпеки програмного забезпечення, вивчення студентами основ стенографічного захисту інформації та особливості побудови інфраструктури відкритих ключів.

Завдання навчальної дисципліни: формування у студентів володіння принципами побудови комплексних систем захисту інформації; вміння розробляти, проводити дослідження та застосовувати механізми щодо забезпечення автентичності, цілісності та конфіденційності в програмно-апаратних, програмних засобах; володіння основами стенографічного захисту інформації, принципами захисту програмного коду від зламу/модифікації; вміння побудови інфраструктури відкритих ключів.

Місце навчальної дисципліни в освітній програмі: ОК 31. НДПП 1.2.19.

Передумови для вивчення дисципліни: " Вища математика ", " Основи криптографічного захисту інформації ", " Прикладна криптологія".

Результати навчання: Уміння організувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. Здатність 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. Здатність виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. Здатність застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. Здатність вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. - Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. 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. Здійснювати аналіз та мінімізацію ризиків обробки 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.

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

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

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	інд	с.р.		л	п	сем	інд	с.р.
Модуль 1												
Змістовий модуль 1. Основи сертифікації відкритих ключів.												
Тема 1. Вступ до інфраструктури відкритих ключів та системи ЕЦП.	**14**	2	1	1		10	**13**	1	1	1		10
Тема 2. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів.	**14**	2	1	1		10	**12**		1	1		10
Тема 3. Життєві цикли особистих ключів та сертифікатів відкритих ключів. Формат(и) особистих ключів.	**17**	4	1	2		10	**18**	1	1	1		15
Тема 4. Обслуговування сертифікатів відкритих ключів.	**15**	2	1	2		10	**17**		1	1		15
Разом за змістовим модулем 1	**60**	**10**	**4**	**6**		**40**	**60**	**2**	**4**	**4**		**50**
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.	**15**	2	2	1		10	**22**	1		1		20
Тема 6. Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації	**17**	4	2	1		10	**13**	1	1	1		10
Тема 7. Валідація (перевірка) шляхів сертифікації при наданні електронних довірчих послуг.	**17**	4	2	1		10	**22**		1	1		20
Тема 8. Стандартизація у галузі ІВК та надання електронних довірчих послуг.	**24**	4	2			18	**12**		1	1		10
Тема 9. Класифікація протоколів ІВК, особливості,застосування та аналіз.	**15**	2	2	1		10	**19**		1			18
Разом за змістовим модулем 2	**88**	**16**	**10**	**4**		**58**	**88**	**2**	**4**	**4**		**78**
Модуль 2												
ІНДЗ	**2**				**2**		**2**				**2**	
Усього годин	**150**	**26**	**14**	**10**	**2**	**98**	**150**	**4**	**8**	**8**	**2**	**128**

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Порівняльний аналіз національної та міжнародної нормативно – правової бази в частині ІВК (ЕЦП) та напрями удосконалення і розвитку національної бази.	4
2	Генерування та використання асиметричних пар ключів ЕЦП та НШ у прикладних системах.	2
3	Технічні специфікації та формати даних ЕЦП(ІВК), сутність, стандартизація та застосування	4
	Усього	10

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Нормативно – правова база створення та застосування національної системи ЕЦП (ІВК). Призначення та застосування національної системи ЕЦП.	2
2	Дослідження стандартизованих криптографічних протоколів ЕЦП та НШ по критеріям стійкості та складності.	2
3	Дослідження механізмів створення запиту та виготовлення сертифікатів відкритих ключів національної системи ЕЦП	1
4	Дослідження механізмів генерування асиметричних пар ключів на робочих станціях та на відокремлених пунктах реєстрації	2
5	Аналіз стану та дослідження механізмів забезпечення криптографічної живучості в ІВК (системі ЕЦП)	1
6	Дослідження бізнес процесів акредитованого центру сертифікації ключів. Регламент АЦСК та його застосування	2
7	Формати сертифікатів відкритих ключів та списків відкликаних сертифікатів. Дослідження активності ЦСК та вимоги до пропускної здатності ЦСК	2
8	Аналіз процесів та процедур розгортання ЦСК для застосування в комерційних чи банківських системах	2
	Усього	14

7. 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	10
3	Принципи побудування та функціонування національної системи ЕЦП. Центри сертифікації, вимоги до них та застосування	10
4	Механізми генерування асиметричних пар ключів на робочих станціях та на відокремлених пунктах реєстрації. Принципи реалізації ІВК	10
5	Сертифікати відкритих ключів. Прикладні формати сертифікатів та технічні специфікації для ІВК.	10
6	Механізми виготовлення та обслуговування сертифікатів відкритих ключів в центрах сертифікації ключів	10
7	Шляхи сертифікації в системі ІВК (ЕЦП). Особливості застосування при наданні електронних довірчих послуг	10
8	Стандартизація у галузі ІВК. Нормативні та нормативно-технічні документу з регулювання діяльності ЦСК (АЦСК)	10
9	Криптографічні протоколи для надання в системі ЕЦП (ІВК) послуг цілісності, неспростовності, доступності та неспростовності	10
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.	10
	Усього	98

8. Індивідуальні завдання

Підготовка тез доповіді на конференції/статті з обраної теми. Вирішення типових завдань за темами змістових модулів.

9. Методи навчання

Викладання дисципліни здійснюється через лекційні та практичні заняття, індивідуальні та групові консультації, самостійну роботу студентів з виконання практичних завдань по кожній темі по індивідуальним варіантам, захист практичних робіт, тестування. Усі теми дисципліни згруповані у 2 змістових модуля.

10. 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 недостатньо 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.

11. Засоби оцінювання

Поточний контроль знань студентів здійснюється за допомогою тестів, опитувань по темам, захисту звітів про виконання лабораторних робіт. Модульний контроль здійснюється із застосуванням тестів. Підсумковий контроль здійснюється у формі екзамену.

Завданням поточного контролю знань студентів є перевірка розуміння та запам'ятовування певного теоретичного матеріалу, умінь самостійної роботи зі спеціальною літературою, набуття практичних навичок роботи з ПК і окремими програмними засобами, вміння пояснити і захистити свою роботу.

12. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота											Екзамен	Сума в балах
Змістовний модуль 1					Змістовний модуль 2							
Т 1	Т 2	Т 3	Т 4	Тести	Т 5	Т 6	Т 7	Т 8	Т 9	Тести		
3	3	3	3	10	4	4	4	4	4	8	50	100

Т1, Т2, ... – змістові теми

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**		
70 - 74	**D**	задовільно	
64 - 73	**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

13. Інструменти, обладнання та програмне забезпечення

Під час викладання дисципліни для занять використовується лабораторна база комп’ютерних класів МДУ, які обладнано мережею комп’ютерів платформи x86.

14. Рекомендовані джерела інформації

Основні:

1Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.

2Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / [О. В. Потій, А. В. Лєншин, Л. С. Сорока, В. І. Єсін і ін.]. – Дніпропетровськ: Академія митної служби України, 2011. – 202с.

3Потій О.В., Іщенко Ю.М., Лєншин А.В. Текст лекцій з дисципліни «Побудова та розгортання інфраструктури відкритих ключів», Харків, ХНУРЕ, 2009 р.

4Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.

5Горбатов В.С. Основы технологии PKI / В.С. Горбатов, О.Ю. Полянская. – М. : Горячая линия – Телеком, 2004. – 246с.

Додаткові:

1. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти управління ключами / О.В. Потій. – Х. : ХНУРЕ, 2002. – 80 с.

2. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти механізмів безпеки/ О.В. Потій. – Х. : ХНУРЕ, 2001. – 80 с.

3. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.

4. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.

5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852- IX

6. Постанова Кабінету Міністрів України від 28.10.04.№1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади».

7. ITU-T Recommendation X.509. Information Technology - Open Systems Interconnection - The Directory Public Key and Attribute Certificate Frameworks. June 2000 (документ эквивалентен ISO/IEC 9594-8 Directory Services, 2000)..