МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра математичних методів та системного аналізу

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.5 Прикладна криптологія
(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

Прикладна криптологія

(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

(підпис) (Т.В. Шабельник) (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">ОПП
Кібербезпека
(назва)
Спеціальність
125 Кібербезпека
(код та найменування спеціальності)</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>3-й</td><td>3-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 - 90</td><td>5-й</td><td>5-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:
бакалавр</td><td colspan="2">Лекції</td></tr>
<tr><td>20 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>16 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>14 год</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>98 год.</td><td>130 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">залік</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: формуванні у студентів розуміння основ прикладної криптології, вміння застосовувати криптографічні методи дешифрування, вміння застосовувати методи зламу інформації, ознайомлення студентів з актуальними питаннями впливу шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому.

Завдання навчальної дисципліни: придбання знань в області криптології з урахуванням сучасного стану та прогнозу розвитку методів захисту за зламу; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

Місце навчальної дисципліни в освітній програмі: ОК17 1. НДПП 1.2.5.

Передумови для вивчення дисципліни: "Дискретна математика", "Програмування", " Архітектура та програмне забезпечення комп'ютерних систем ", "Алгоритми та структури даних"..

Відповідно ОП дисципліна сприяє досягненню таких навчальних результатів:

Результати навчання	Шифр результату навчання
вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень	РН14
використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій	РН15
реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів	РН16
використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів	РН18
застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	РН19
вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах	РН27
застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем	РН31
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	РН35

встановленої політики інформаційної і\або кібербезпеки	
забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур	РН41
вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	РН47
виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах	РН 48

3. Програма навчальної дисципліни

Змістовий модуль 1. Математичні методи та симетричні криптографічні перетворення.

Тема 1. Теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії.

Тема 2. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.

Тема 3. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.

Тема 4. Основи теорії секретних систем (конфіденційності).

Тема 5. Симетричні криптографічні перетворення та їх властивості.

Тема 6. Джерела ключів та ключової інформації, вимоги до них

Змістовий модуль 2. Асиметричні криптосистеми та методи автентифікації.

Тема 7. Вступ в теорію асиметричних крипто перетворень

Тема 8. Асиметричні крипто перетворення в групах точок еліптичних кривих.

Тема 9. Джерела ключів асиметричних криптосистем та вимоги до них.

Тема 10. Методи та механізми автентифікації в криптосистемах.

Тема 11. Методи та механізми захисту від несанкціонованого доступу.

Змістовий модуль 3. Криптографічні механізми та протоколи.

Тема 12. Криптографічні механізми та протоколи управління ключами. Криптографічні механізми та протоколи автентифікації. Синтез та аналіз криптографічних протоколів. Квантова криптографія та крипто аналіз.

Тема 13. Електронні цифрові підписи з додатком. Електронні цифрові підписи з відновлення повідомлень. Властивості та основи застосування електронних цифрових підписів.

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. Математичні методи та симетричні криптографічні перетворення												
Тема 1. Теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії.	**7**	2				5	**7**	1				6
Тема 2. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.	**10**	2	2	1		5	**10**		1			9
Тема 3. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.	**9**	2	1	1		5	**9**					9
Тема 4. Основи теорії секретних систем (конфіденційності).	**7**	2	2	1		2	**7**	1				6
Тема 5. Симетричні криптографічні перетворення та їх властивості	**2**		1	1			**2**		1			1
Тема 6. Джерела ключів та ключової інформації, вимоги до них	**4**			1		3	**4**					4
Разом за змістовим модулем 1	**39**	**8**	**6**	**5**		**20**	**39**	**2**	**2**			**35**
Змістовий модуль 2. Асиметричні криптосистеми та методи автентифікації.												
Тема 7. Вступ в теорію асиметричних крипто перетворень	**13**	2	2	1		8	**13**		1			12
Тема 8. Асиметричні крипто перетворення в групах точок еліптичних кривих	**14**	1	1	2		10	**14**	1	1	1		11
Тема 9. Джерела ключів асиметричних криптосистем та вимоги до них	**15**	2	2	1		10	**15**		1			14
Тема 10. Методи та механізми автентифікації в криптосистемах.	**15**	1	2	2		10	**15**	1		1		13
Тема 11. Методи та механізми захисту від несанкціонованого	**14**	2	1	1		10	**14**		1			13

доступу												
Разом за змістовим модулем 2	**71**	**8**	**8**	**7**		**48**	**71**	**2**	**4**	**2**		**63**
Змістовий модуль 3. Криптографічні механізми та протоколи												
Тема 12. Криптографічні механізми та протоколи управління ключами. Криптографічні механізми та протоколи автентифікації. Синтез та аналіз криптографічних протоколів. Квантова криптографія та крипто аналіз	**24**	2	1	1		20	**24**	2		2		20
Тема 13. Електронні цифрові підписи з додатком. Електронні цифрові підписи з відновлення повідомлень. Властивості та основи застосування електронних цифрових підписів	**14**	2	1	1		10	**14**	2		2		10
Разом за змістовим модулем 3	**38**	**4**	**2**	**2**		**30**	**38**	**4**		**4**		**30**
Модуль 2												
ІНДЗ	**2**				**2**						**2**	
Усього годин	**150**	**20**	**16**	**14**	**2**	**98**	**150**	**8**	**6**	**6**	**2**	**128**

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз методів скалярного множення в групі точок еліптичних кривих, афінне та проективне подання точок еліптичних кривих, порівняльний аналіз складності операцій додавання та подвоєння точок еліптичних кривих для різних подань	2
2	Аналіз методів криптографічних перетворень, критерії та показники оцінки якості крипто перетворень, умови реалізації безумовно стійких, обчислювально стійких та ймовірно стійких шифрів	2
3	Аналіз методів симетричних крипто перетворень, блокові та потокові симетричні шифри та методичні основи їх порівняння. Елементарні шифри та їх властивості	4
4	Класифікація цифрових підписів. Цифрові підписи з додатком. Основні загрози та протидія їм. Оцінка стійкості цифрових підписів з додатком. Стандартизація цифрових підписів з додатком	2
5	Аналіз протоколів управління ключами. Основні механізми та протоколи. Критерії та показники оцінки та порівняльного аналізу. Стандартизація протоколів управління ключами	4
6	Методи та системи крипто аналізу асиметричних криптосистем. Складність крипто аналізу перетворень типу цифровий підпис та направлене шифрування групі точок еліптичних кривих	2
	Усього	16

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Джерела ключів. Методи та засоби формування випадкових та псевдовипадкових послідовностей. Дослідження властивостей випадкових та псевдовипадкових послідовностей	2
2	Дослідження властивостей асиметричних крипто перетворень в групі точок еліптичних кривих	2
3	Розроблення програмних моделей та дослідження перспективних криптографічних перетворень типу електронний цифровий підпис	2
4	Протоколи розподілу таємниці. Класифікація та вимоги до протоколів розподілу таємниці. Методи розподілу та підтвердження таємниці. Синтез та аналіз	2

	криптографічних протоколів	
5	Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих	4
6	Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок гіпер еліптичних кривих	2
	Усього	14

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Математичні основи криптології	10
2	Симетричні криптографічні системи погроз	10
3	Асиметричні криптографічні системи	10
4	Методи автентифікації інформації	10
5	Цифровий підпис та його властивості	10
6	Криптографічні протоколи	10
7	Криптографічний аналіз асиметричних криптосистем	10
8	Криптографічний аналіз симетричних криптосистем	10
9	Виконання курсової роботи	19
	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 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.

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													Сума в балах
Змістовний модуль 1						Змістовний модуль 2					Змістовний модуль 3		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	
7	7	7	8	9	7	7	8	7	8	9	8	8	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:

1 Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний підручник. Харків, ХНУРЕ, 2011 р.

2 Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2011 р.

3 Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

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

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

Додаткова:

1. Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с.
2. Бембо Мао. Современная криптографія. Теорія и практика. Москва. 2005.
3. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
4. Б. Шнайер . Безопасность данных в цифровом мире. Изд. Питер. Харьков. 2003 г. 367 с.
5. В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”. К. 2001. 669 с.
6. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Також «Введение в криптографию» под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html).
7. А. Менезис, П. Ван Аршот, С. Ватсон. Руководство по прикладной криптографии CRC Press, 1997, электронная копия, 662 с.
8. Бессалов А., Телиженко А. Криптосистемы на эллиптических кривых. – К.: «Політехніка», 2004. – 224 с.
9. Радіотехніка № 114, 119, 126, 134, 141, 142,145.Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000- 2008 рр.
10. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» №2- 2006; №2, №3-2007, №3- 2008, №3 – 2009, № 3 – 2010, №2 – 2011рр.