МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра системного аналізу та інформаційних технологій

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.7 Криптологія
(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
Криптологія 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

1. Опис навчальної дисципліни

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, спеціальність, освітній рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td>Кількість кредитів – 6</td><td>Галузь знань
12 Інформаційні технології
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">ОП
125 Кібербезпека
(шифр і назва)

Спеціальність
Кібербезпека</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів –2</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 - 180</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">Рівень вищої освіти:

бакалавр</td><td colspan="2">Лекції</td></tr>
<tr><td>26 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>26 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год</td><td>16 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>108 год.</td><td>144 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2"></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 40 %,

для заочної форми навчання 20%

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, системта засобів здійснення захисту інформації у системах та мережах.

Місце навчальної дисципліни в освітній програмі: ОК16 1. НДПП 1.2.7.

Передумови для вивчення дисципліни: "Дискретна математика", "Програмування", "Алгоритми та структури даних".

Компетентності та результати навчання:
ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
КЗ2. Знання та розуміння предметної області та розуміння професії.
КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

РН6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
РН14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
РН15 Використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій
РН16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів
РН18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
РН19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації

в інформаційно-телекомунікаційних системах;
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;
РН41 Забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН47 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
РН48 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. Математичні методи та симетричні криптографічні перетворення.

Тема 1. Методи та механізми захисту від несанкціонованого доступу.

Тема 2. Основи теорії секретних систем (конфіденційності).

Тема 3. Методи та механізми автентифікації в криптосистемах.

Тема 4. Групи, кільця та скінченні поля Галуа, особливості застосування в криптографії.

Тема 5. Симетричні криптографічні перетворення та їх властивості. Сучасні стандарти симетричних шифрів.

Тема 6. Сучасні потокові шифри.

Тема 7. Джерела ключів та ключової інформації, вимоги до них

Змістовий модуль 2. Асиметричні криптосистеми та методи автентифікації.

Тема 8. Вступ в теорію асиметричних крипто перетворень.

Тема 9. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.

Тема 10. Асиметричні криптоперетворення в групах точок еліптичних кривих.

Тема 11. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.

Тема 12. Джерела ключів асиметричних криптосистем та вимоги до них.

Тема 13. Сучасні методи та механізми автентифікації в криптосистемах.

3. 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	лаб	інд	с.р.
Змістовий модуль 1. Математичні методи та симетричні криптографічні перетворення												
Тема 1. Методи та механізми захисту від несанкціонованого доступу.	**11**	1				10	**12**	2				10
Тема 2. Основи теорії секретних систем (конфіденційності).	**13**	2	2	1		8	**12**					12
Тема 3. Методи та механізми автентифікації в криптосистемах.	**16**	2	4	2		8	**12**		2	2		8
Тема 4. Групи, кільця та скінченні поля Галуа, особливості застосування в криптографії.	**14**	2	2	2		8	**13**	1	2	2		8
Тема 5. Симетричні криптографічні перетворення та їх властивості. Сучасні стандарти симетричних шифрів.	**14**	2	2	2		8	**13**	1	2	2		8
Тема 6. Сучасні потокові шифри.	**13**	2		1		10	**13**	1				12
Тема 7. Джерела ключів та ключової інформації, вимоги до них	**12**	2				10	**11**	1				10
Разом за змістовим модулем 1	**93**	**13**	**10**	**8**		**62**	**82**	**6**	**6**	**6**		**68**
Змістовий модуль 2. Асиметричні криптосистеми та методи автентифікації.												
Тема 8. Вступ в теорію асиметричних криптоперетворень	**14**	2	2	2		8	**14**					14
Тема 9. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.	**16**	2	4	2		8	**15**	2	1	2		10
Тема 10. Асиметричні крипто перетворення в групах точок еліптичних кривих	**18**	4	4	2		8	**16**	1	1	2		12
Тема 11. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.	**12**	2	2	2		6	**15**		1			14
Тема 12. Джерела ключів	**14**	2	2	2		8	**18**	1		4		13

асиметричних криптосистем та вимоги до них.												
Тема 13. Сучасні методи та механізми автентифікації в криптосистемах.	**13**	1	2	2		8	**14**		1			13
Разом за змістовим модулем 2	**57**	**13**	**16**	**12**		**46**	**92**	**4**	**4**	**6**		**76**
ІНДЗ												
Усього годин	**150**	**26**	**26**	**20**		**108**	**150**	**8**	**10**	**10**		**144**

4. Теми практичних занять

№ з/п	Назватеми	Кількість годин	
1	Аналіз методів скалярного множення в групі точокеліптичних кривих, афінне та проективне подання точок еліптичних кривих, порівняльний аналіз складності операцій додавання та подвоєння точокеліптичних кривих для різних подань	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
2	Аналіз методів криптографічних перетворень, критерії та показники оцінки якості крипто перетворень, умови реалізації безумовно стійких, обчислювально стійких та ймовірно стійких шифрів	6	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
3	Аналіз методів симетричних крипто перетворень, блокові та потокові симетричні шифри та методичні основи їх порівняння. Елементарні шифри та їхвластивості	6	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
4	Класифікація цифрових підписів. Цифрові підписи здодатком. Основні загрози та протидія їм. Оцінка стійкості цифрових підписів з додатком. Стандартизація цифрових підписів з додатком	6	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
5	Аналіз протоколів управління ключами. Основні механізми та протоколи. Критерії та показники оцінкита порівняльного аналізу. Стандартизація протоколів управління ключами	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
6	Методи та системи крипто аналізу асиметричних криптосистем. Складність крипто аналізу перетвореньтипу цифровий підпис та направлене шифрування групі точок еліптичних кривих	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
	Усього	26	

5. Теми лабораторних занять

№	Назватеми	Кількість	

з/п		годин	
1	Джерела ключів. Методи та засоби формування випадкових та псевдовипадкових послідовностей. Дослідження властивостей випадкових та псевдовипадкових послідовностей	2	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
2	Дослідження властивостей асиметричних крипто перетворень в групі точок еліптичних кривих	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
3	Розроблення програмних моделей та дослідження перспективних криптографічних перетворень типуелектронний цифровий підпис	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
4	Протоколи розподілу таємниці. Класифікація та вимоги до протоколів розподілу таємниці. Методи розподілу та підтвердження таємниці. Синтез та аналіз криптографічних протоколів	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
5	Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок еліптичних кривих	4	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
6	Методи та алгоритми крипто аналізу криптографічних перетворень в групі точок гіпер еліптичних кривих	2	РН6,РН14, РН15, РН16, РН18, РН19, РН27, РН31, РН35, РН41, РН47, РН48
	Усього	20	

6. Самостійна робота

№ з/п	Назватеми	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	Підготовка до заліку	28
	Усього	108

8. Методи навчання

Як *форми контролю якості одержаних знань* застосовуються :

- *вхідний контроль* знань з інформатики 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.

9. Засоби діагностики результатів навчання

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

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.

10. Розподіл балів, які отримують студенти

Вид роботи	Кіль-кість го-дин	Обсяг креди-тів	Кіль-кість ба-лів
Змістовий модуль 1. Математичні методи та симетричні криптографічні перетворення			
Тема 1. Методи та механізми захисту від несанкціонованого доступу.			
лекційні	1	0,03	1
Тема 2. Основи теорії секретних систем (конфіденційності).			
лекційні	2	0,07	1
практичні заняття	2	0,07	4
лабораторні заняття	1	0,03	4
Тема 3. Методи та механізми автентифікації в криптосистемах.			
лекційні	2	0,07	1
практичні заняття	4	0,14	4
лабораторні заняття	2	0,07	4
Тема 4. Групи, кільця та скінченні поля Галуа, особливості застосування в криптографії.			
лекційні	2	0,07	1
практичні заняття	2	0,07	3
лабораторні заняття	2	0,07	3
Тема 5. Симетричні криптографічні перетворення та їх властивості. Сучасні стандарти симетричних шифрів.			
лекційні	2	0,07	1
практичні заняття	2	0,07	3
лабораторні заняття	2	0,07	3
Тема 6. Сучасні потокові шифри.			
лекційні	2	0,07	1
лабораторні заняття	1	0,03	3
Тема 7. Джерела ключів та ключової інформації, вимоги до них			
лекційні	2	0,07	1
Змістовий модуль 2. Асиметричні криптосистеми та методи автентифікації.			
Тема 8. Вступ в теорію асиметричних криптоперетворень			
лекційні	2	0,07	1
практичні заняття	2	0,07	3

лабораторні заняття	2	0,07	3
Тема 9. Еліптичні та гіпереліптичні групи, основи застосування в криптографії.			
лекційні	2	0,07	1
практичні заняття	4	0,28	3
лабораторні заняття	2	0,07	3
Тема 10. Асиметричні крипто перетворення в групах точок еліптичних кривих			
лекційні	4	0,13	1
практичні заняття	4	0,13	3
лабораторні заняття	2	0,07	3
Тема 11. Бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії.			
лекційні	2	0,07	1
практичні заняття	2	0,07	4
лабораторні заняття	2	0,07	4
Тема 12. Джерела ключів асиметричних криптосистем та вимоги до них.			
лекційні	2	0,07	1
практичні заняття	2	0,07	4
лабораторні заняття	2	0,07	4
Тема 13. Сучасні методи та механізми автентифікації в криптосистемах.			
лекційні	1	0,03	1
практичні заняття	2	0,07	4
лабораторні заняття	2	0,07	4
Тези/наук. стаття			14
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.
Перелік програмного забезпечення:
Visual Studio, PyCharm, NetBeans, Eclipce, Idea Studio.

13. Рекомендовані джерела інформації:

Обов'язкова література:

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.-656с.

Додаткова:

6. Радіотехніка № 114, 119, 126, 134, 141, 142,145.Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000- 2008 рр.

14. Політика навчальної дисципліни

Політика навчальної дисципліни «Прикладна криптологія» 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 практичних 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 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.