**МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**Кафедра математичних методів та системного аналізу**


# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДЗП 1.1.11 Основи криптографічного захисту інформації
(шифр і назва навчальної дисципліни)

Освітньо-професійна програма Кібербезпека, Системний аналіз
(назва)

Спеціальність 125 Кібербезпека,124 Системний аналіз
(код та найменування спеціальності)

Спеціалізація _____
(назва спеціалізації)

Факультет Економіко-правовий
(назва факультету)

2020 – 2021 рік

Робоча програма з дисципліни

Основи криптографічного захисту інформації

(назва навчальної дисципліни)

для студентів ОП Кібербезпека, ОП Системний аналіз
за спеціальністю (напрямом підготовки) 125 Кібербезпека, 124 Системний аналіз

Розробники:
Неласа Г.В. доцент кафедри математичних методів та системного аналізу
Морозова А.О. асистент кафедри математичних методів та системного 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)

© Неласа Г.В. 2020 рік
© Морозова А.О. 2020 рік
© МДУ, 2020 рік

## 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 – 3</td><td>Галузь знань:<br>12 Інформаційні технології<br>(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">ОПП<br>Системний аналіз<br>(назва)<br>Спеціальність<br>124 Системний аналіз<br>(код та найменування спеціальності)</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<br>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:<br>аудиторних -4<br>самостійної роботи студента – 8</td><td rowspan="11">Освітній рівень:<br>магістр</td><td colspan="2">Лекції</td></tr>
<tr><td>20 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>10 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td></td><td>.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td>77 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2">1 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:** формування сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах, починаючи з криптографічних методів захисту інформації; формуванні у студентів розуміння основ інформаційної безпеки, вміння застосовувати криптографічні методи шифрування, вміння проектувати підсистеми захисту комп'ютерних систем, вміння застосовувати методи шифрування інформації для передачі у мережі, вміння розробляти парольні захищенні системи, ознайомлення зі шляхами використовування управління доступом різними методами; ознайомлення студентів з актуальними питаннями впливу комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому, ознайомлення з методами захисту мережевої інформації.

**Завдання навчальної дисципліни:** надання основних відомостей з принципів протидії спробам несанкціонованого доступу до інформації з боку сторонніх осіб; придбання знань в області захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів; освоєння засобів аналізу погроз інформаційній безпеці; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

**Місце навчальної дисципліни в освітній програмі:** ОК 11. НДЗП 1.1.11.

**Передумови для вивчення дисципліни:** "Дискретна математика", "Програмування", " Архітектура та програмне забезпечення комп'ютерних систем ", "Комп'ютерні мережі"..

Відповідно ОП дисципліна сприяє досягненню таких навчальних результатів:

| Результати навчання | Шифр результату навчання |
|---|---|
| критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності | РН6 |
| 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 |
| 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 | РН48 |

## 3. Програма навчальної дисципліни

### Змістовий модуль 1. Принципи безпеки та захисту інформації в ПЗ.

Тема 1. Загрози безпеки та методи захисту. Основні шляхи витоку інформації та несанкціонованого доступу в каналах телекомунікацій.

Вступ. Предмет та задачі курсу. Основні визначення та термінологія. Література, що рекомендується.

Тема 2. Політика захисту інформації. Свідомість працівників. Окреслення небезпеки і потенційно можливих атак.

Тема 3. Нормативна і правова бази захисту інформації в системах та мережах телекомунікації України. Законодавча, нормативно-методична, наукова, нормативно-правова бази України із забезпечення інформаційної безпеки в системах телекомунікацій.

Тема 4. Аналіз уразливостей інформаційних систем та оцінка ризиків.

### Змістовий модуль 2. Основи побудови систем захисту інформації в ПЗ.

Тема 5. Криптографічний захист інформації. Основні принципи шифрування. Стандарти шифрування. Сучасні криптографічні бібліотеки

Тема 6. Криптографічні системи з закритим ключем. Блокові шифри. Потокові шифри.

Тема 7. Односторонні функції. Ґеш-функції. Криптографічні системи з відкритим ключем

Тема 8. Протоколи цифрового підпису на еліптичних кривих.

Тема 9. Методи створення високозахищених та алгоритмічно безпечних програм для використання в системах критичних додатків. Способи захисту коду програми від дизасемблювання.

Тема 10. Захищені операційні системи. Схема контролю доступу до ресурсів

Тема 11. Безпека Internet - технологій. Організація віртуальних приватних мереж

Тема 12. Комп’ютерні віруси. Класифікація. Методи протидії

## 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. Принципи безпеки та захисту інформації в ПЗ.** | | | | | | | | | | | | |
| Тема 1. Загрози безпеки та методи захисту. Основні шляхи витоку інформації та несанкціонованого доступу в каналах телекомунікацій. | **7** | 2 | | | | 5 | 7 | 1 | | | | 6 |
| Тема 2. Політика захисту інформації. Свідомість працівників. Окреслення небезпеки і потенційно можливих атак. | **9** | 2 | 2 | | | 5 | 9 | 1 | 1 | | | 7 |
| Тема 3. Нормативна і правова бази захисту інформації в системах та мережах телекомунікації України. Законодавча, нормативно-методична, наукова, нормативно-правова бази України із забезпечення інформаційної безпеки в системах телекомунікацій. | **8** | 2 | 1 | | | 5 | 8 | 1 | 1 | | | 6 |
| Тема 4. Аналіз уразливостей інформаційних систем та оцінка ризиків. | **9** | 2 | 2 | | | 5 | 9 | | 1 | | | 8 |
| Разом за змістовим модулем 1 | **33** | **8** | **5** | | | **20** | **33** | **3** | **3** | | | **27** |
| **Змістовий модуль 2. Основи побудови систем захисту інформації в ПЗ.** | | | | | | | | | | | | |
| Тема 5. Криптографічний захист інформації. Основні принципи шифрування. Стандарти шифрування. Сучасні криптографічні бібліотеки | **7** | 2 | | | | 5 | **7** | | | | | 7 |
| Тема 6. Криптографічні системи з закритим ключем. Блокові шифри. Потокові шифри | **7** | 1 | 1 | | | 5 | **7** | 1 | | | | 6 |
| Тема 7. Односторонні функції. Ґеш-функції. Криптографічні системи з відкритим ключем | **8** | 2 | 1 | | | 5 | **8** | | 1 | | | 7 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Тема 8. Протоколи цифрового підпису на еліптичних кривих. | **6** | 1 | | | | 5 | **6** | 1 | | | | 5 |
| Тема 9. Методи створення високозахищених та алгоритмічно безпечних програм для використання в системах критичних додатків. Способи захисту коду програми від дизасемблювання | **8** | 2 | 1 | | | 5 | **8** | | 1 | | | 7 |
| Тема 10. Захищені операційні системи. Схема контролю доступу до ресурсів | **7** | 2 | 1 | | | 4 | **7** | 1 | | | | 6 |
| Тема 11. Безпека Internet - технологій. Організація віртуальних приватних мереж | **6** | 1 | | | | 5 | **6** | | 1 | | | 5 |
| Тема 12. Комп'ютерні віруси. Класифікація. Методи протидії | **7** | 1 | 1 | | | 5 | **7** | | | | | 7 |
| Разом за змістовим модулем 2 | **56** | **12** | **5** | | | **39** | **56** | **3** | **3** | | | **50** |
| **Модуль 2** | | | | | | | | | | | | |
| ІНДЗ | **1** | | | | **1** | | **1** | | | | **1** | |
| **Усього годин** | **90** | **20** | **10** | | **1** | **59** | **90** | **6** | **6** | | **1** | **77** |

## 5. Теми практичних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Базові шифри. Частотний криптоаналіз | 2 |
| 2 | Режими шифрування блокових шифрів | 2 |
| 3 | Криптографія з відкритим ключем. Функція ґешування | 2 |
| 4 | Криптографічні перетворення на еліптичних кривих | 2 |
| 5 | Стеганографічний захист | 2 |
| | Усього | 10 |

## 6. Самостійна робота

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Віртуальні приватні мережі. | 5 |
| 2 | Архітектура і конфігурація Farewall. | 5 |
| 3 | Захищені операційні системи. | 5 |
| 4 | Смарт-карти: архітектура, технології, галузі застосування. | 5 |
| 5 | Банківські технології. | 5 |
| 6 | Комп’ютерні віруси. Класифікація. Методи протидії. | 5 |
| 7 | Захищені бази даних. | 5 |
| 8 | Система безпеки Windows XP. | 5 |
| 9 | Безпека Internet - бізнесу. | 5 |
| 10 | Технічні засоби захисту інформації. | 5 |
| | Усього | 50 |

## 7. Індивідуальні завдання

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

## 8. 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.

## 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. 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.

## 11. Розподіл балів, які отримують студенти

| Поточне тестування та самостійна робота | | | | | | | | | | | | | | Сума в балах |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Змістовний модуль 1 | | | | | Змістовний модуль 2 | | | | | | | | | |
| Т1 | Т2 | Т3 | Т4 | Тести | Т5 | Т6 | Т7 | Т8 | Т9 | Т10 | Т11 | Т12 | Тести | |
| 2 | 3 | 5 | 5 | 10 | 8 | 6 | 5 | 8 | 8 | 8 | 7 | 5 | 20 | 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 |

## 12. 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.

## 13. Рекомендовані джерела інформації

**Основні:**

1 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. –368с. рос.

2 Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: Горячая линия, 2001. – 120с. рос. (20)

3 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и свіязь, 2001. – 376с. рос.

4 Жельников В. Криптография от папируса до компьютера. М.: ABF , 1996 – 336с.

5 Подбельский В.В., Фомин С.С. Программирование на языке Си. М:Финансы и статистика, 2002 .-600с. рос.(є електронна версія документу)

6 Фергюсон Н., Шнайер Б. Практическая криптография – М.: Диалектика, 2005. – 424 с.

7 Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 168 с.

**Додаткова:**

1. Березин Б.И., Березин С.Б. Начальный курс С и С++ . М.:ДИАЛОГ-МИФИ, 2000.-288с. рос.

2. Петраков А.В. «Основы практической защиты информации» – М.: Радио и связь, 1999. – 368с.

3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации / Под ред. Ю.С. Ковтанька – К.:Изд-во Юниор, 2003. – 504с.

**4.** Лидл Р., Нидеррайтер Х. Конечные поля. – М.: Мир, 1988.