МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра математичних методів та системного аналізу

ЗАТВЕРДЖУЮ
Завідувач кафедри ММСА
_____ Т.В. Шабельник
«__» _____ 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.6. Теорія інформації та кодування

(шифр і назва навчальної дисципліни)

напрям підготовки _____ _____
(шифр і назва напряму підготовки)

спеціальність 124 Системний аналіз, 125 «Кібербезпека»
(шифр і назва спеціальності)

спеціалізація _____
(назва спеціалізації)

факультет _____економіко-правовий_____
(назва факультету)

м. Маріуполь - 2020 рік

Робоча програма з «Теорія інформації та кодування»
(назва навчальної дисципліни)
для студентів спеціальності ОП Системний аналіз, ОП Кібербезпека
за спеціальністю (напрямом підготовки) 125 Кібербезпека, 124 Системний аналыз

Розробники:
Кривенко О.В., кандидат технічних наук, доцент, доцент кафедри інформатики
(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робоча програма затверджена на засіданні кафедри математичних методів та системного аналізу
Протокол № 1 від « 27 » серпня 2020 року

Завідувач кафедри математичних методів та системного аналізу

(Шабельник Т. В.)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 5</td><td>Галузь знань: 12 Інформаційні технології</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>124 Системний аналіз, 125 «Кібербезпека»</td></tr>
<tr><td>Модулів –</td><td rowspan="5"></td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td><td></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання - вирішення типових завдань за темами змістових модулів</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 150</td><td>1-й</td><td>2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: аудиторних - самостійної роботи студента –</td><td rowspan="10">Освітній ступінь: бакалавр</td><td>24</td><td>8</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>26</td><td>12</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>98</td><td>128</td></tr>
<tr><td colspan="2">Індивідуальні завдання: 2</td></tr>
<tr><td colspan="2">Вид контролю: 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

Метою навчальної дисципліни є вивчення основних методів теорії інформації і кодування, які широко використовуються в сучасних комп'ютерних інформаційних технологіях в різних сферах діяльності людей.

Завданням навчальної дисципліни є надання знань щодо способів та практичних навичок вимірювання кількості інформації, яку несуть в собі будь-які повідомлення, способи ефективного кодування таких повідомлень для передачі, збереження, обробки та відображення в інформаційних системах, забезпечення необхідної надійності їх роботи за рахунок використання завадостійкого кодування.

У результаті вивчення навчальної дисципліни студент повинен

знати:

– основні способи оцінки кількості інформації;

– сучасні алгоритми кодування для джерел повідомлень і передачі даних по каналам зв’язку;

– принципи побудови завадостійких кодів та їх використання в сучасних комп'ютерних інформаційних системах.

вміти:

використовувати основні принципи кодування інформації з метою підвищення ефективності вводу, збереження, обробки та передачі інформації в сучасних інформаційних технологіях.

Місце в структурно-логічній схемі спеціальності – ОК 18 НДПП 1.2.6.

Зв’язок з іншими дисциплінами - навчальна дисципліна «Теорія інформації та кодування» пов’язана з вивченням таких спеціальних дисциплін як «Основи криптографічного захисту інформації», «Прикладна криптологія», «Кібернетична безпека підприємства» (бакалаври).

3. Програма навчальної дисципліни

Змістовий модуль 1 Загальні критерії оцінки і стандарти інформаційної безпеки

Тема 1. Вимоги безпеки до інформаційних систем

Стандарт ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій». Принцип ієрархії: клас – сімейство – компонент – елемент. Функціональні вимоги та вимоги довіри. Інформаційні категорії і категорії безпеки інформаційних систем.

Тема 2. Огляд найбільш поширених методів «злому»

Комплексний пошук можливих методів доступу. Термінали захищеної інформаційної системи.

Тема 3. ПЗ та інформаційна безпека

Огляд сучасного ПЗ. Помилки, що призводять до можливості атак на інформацію. Основні положення по розробці ПЗ. Причини успішної реалізації віддалених загроз в обчислювальних мережах.

Змістовий модуль 2. Основи і додатки криптології

Тема 4. Основні поняття криптології

Основні поняття криптографії. Історія розвитку криптографії та приклади класичних криптосистем. Сучасні криптосистеми. Схеми атаки на шифр.

Тема 5. Стійкість криптографічних систем и алгоритмів

Секретність і стійкість криптосистем та алгоритмів. Інформаційно-теоретичний підхід і підхід на основі теорії складності.

.

Тема 6. Загальна характеристика різних типів шифрів і класів криптосистем

Шифри заміни. Шифри перестановки. Шифри збивання. Шифри з відкритим ключем. Порівняльний аналіз шифрів різних типів.

Тема 7. Схема відкритого розподілу ключів Діффі-Хеллмана

Методи формування псевдовипадкових послідовностей. Принцип роботи схеми відкритого розподілу ключів.

Тема 8. Алгоритм RSA і алгоритм Ель Гамаля роботи криптосистем з відкритим ключем

Алгоритм RSA. Алгоритм Ель Гамаля.

Тема 9. Електронний цифровий підпис

Схема ЕЦП. Реалізації схеми цифрового підпису. Алгоритм підпису і перевірки підпису до повідомлення.

Тема 10. Схеми відкритого розподілу ключів

Відкритий розподіл ключів за алгоритмом Діффі-Хеллмана. Відкритий розподіл ключів за алгоритмом ECKER.

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.
Змістовий модуль 1. Предметна область та основні поняття системного аналізу												
Тема 1. Вимоги безпеки до інформаційних систем	**10**					10	**10**	2		1		7
Тема 2. Огляд найбільш поширених методів «злому»	**10**	2		2		6	**10**	1		1		8
Тема 3. ПЗ та інформаційна безпека	**20**					20	**20**	1		2		17
Разом за змістовим модулем 1	**40**	**2**		**2**		**36**	**40**	**4**		**4**		**32**
Змістовий модуль 2. Основи і додатки криптології												
Тема 4. Основні поняття криптології	**14**	4		4		6	**14**	1		1		12
Тема 5. Стійкість криптографічних систем и алгоритмів	**16**	4		4		8	**16**			1		15
Тема 6. Загальна характеристика різних типів шифрів і класів криптосистем	**16**	4		4		6	**16**	1		1		14
Тема 7. Схема відкритого розподілу ключів Діффі-Хеллмана	**16**	4		6		6	**16**			1		15
Тема 8. Алгоритм RSA і алгоритм Ель Гамаля роботи криптосистем з відкритим ключем	**16**	4			2	10	**16**	1		1		14
Тема 9. Електронний цифровий підпис	**16**	2		4		10	**16**			1		15

Тема 10. Схеми відкритого розподілу ключів	**16**					16	**16**	1		2		13
Разом за змістовим модулем 2	**110**	**22**		**24**	**2**	**62**	**110**	**4**		**8**		**98**
Усього годин	**150**	**24**		**26**	**2**	**98**	**150**	**8**		**12**	**2**	**128**

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Мануальний, напівавтоматичний і автоматичний криптоаналіз найпростіших шифрів: Цезаря і Віженера	2
2	Криптоаналіз побітового шифрування	4
3	Шифри простої заміни, блочні шифри	4
4	Методи розкриття одне і поліалфавітних систем	4
5	Стійкість шифру. Характеристики ключа для шифрування. Оцінка ентропії інформації	4
6	Шифрування інформації методом асиметричною криптографії RSA. Електронний цифровий підпис (ЕЦП).	4
7	Схема відкритого розподілу ключів: Діффі-Хеллмана і ECKER.	4
	Усього	26

5. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Вимоги безпеки до інформаційних систем	10
2	Огляд найбільш поширених методів «злому»	6
3	ПЗ та інформаційна безпека	14
4	Основні поняття криптології	10
5	Стійкість криптографічних систем и алгоритмів	10
6	Загальна характеристика різних типів шифрів і класів криптосистем	10
7	Схема відкритого розподілу ключів Діффі-Хеллмана	10
8	Алгоритм RSA і алгоритм Ель Гамаля роботи криптосистем з відкритим ключем	8
9	Електронний цифровий підпис	10
10	Схеми відкритого розподілу ключів	10
	Усього	98

6. Індивідуальні завдання

Алгоритм RSA і алгоритм Ель Гамаля роботи криптосистем з відкритим ключем.

7. Методи навчання

Викладання дисципліни здійснюється через лекційні та лабораторні заняття, індивідуальні та групові консультації, самостійну роботу студентів з виконанням лабораторних робіт по кожній темі по індивідуальним варіантам, тестування. Усі теми дисципліни згруповані у 2 змістових модуля.

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

Перелік програмного забезпечення: Microsoft Office.

8. Методи контролю

Поточний контроль знань студентів здійснюється за допомогою тестів, опитувань по темам, захисту звітів по лабораторним роботам. 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.

10. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота								Іспит	Сума (в балах)
Змістовий модуль №1		Змістовий модуль №2			Змістовий модуль №3				
Т2	Т3	Т4	Т5	Т6	Т7	Т8	Тест		
5	5	5	5	5	5	5	15	50	100

Т2, Т3, ... – 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

8. Методичне забезпечення:

1) Робоча програма навчальної дисципліни.
2) Конспект лекцій (електронний варіант).
3) Методичні вказівки до самостійних робіт (електронний варіант).
4) Завдання для проведення лабораторних робіт (електронний варіант).
5) Тестові завдання для проведення поточного модульного контролю.

10. Рекомендована література:

Основна:

1. Воронков Б. Н. Элементы теории чисел и криптозащита: учебное пособие / Б. Н. Вороноков, А. С. Щеголеватых. – Воронеж: Изд-во ВГУ, 2008. – 88 с.

2. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности / А. Ю. Щербаков. – М. : Издательство Молгачева С. В., 2001.

3. Криптографическая защита информации в информационных системах : курс лекций / И. Д. Горбенко. – Харьков : ХНУРЭ, 2002.

4. Галатенко В. А. Основы информационной безопасности / В. А. Галатенко. – М. : Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2003.

5. Будко В. Н. Информационная безопасность и защита информации : конспект лекций / В. Н. Будко. – Воронеж : Изд-во ВГУ, 2003. – 86 с.

6. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / В. А. Герасименко. – М. : Энергоатомиздат, 1994.

7. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. – СПб. : БХВ – Санкт-Петербург, 2000. – 384 с.

8. Аскеров Т. М. Защита информации и информационная безопасность: учебное пособие / под общей ред. К. И. Курбакова. – М.: Рос. экон. Академия, 2001. – 387с.

9. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Машок. – М.: ООО «Инкомбук», 1997

10. Дмитриевский Н. П. Информационная безопасность. Борьба с компьютерными вирусами и другими вредоносными программами: учебное пособие / Н. П. Дмитриевский. – М.: МИФИ, 1993.

11. Мельников В. Защита информации в компьютерных системах / В. Мельников. – М.: Финансы и статистика: «ЭЛЕКТРОНИНФОРМ», 1997. – 364 с.

12. Петров В. А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: учебное пособие / В. А. Петров, А. С. Пискарев, А. В. Шеин. – 2-е изд., испр. и доп. – М.: МИФИ, 1995.

Додаткова:

13. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1998. – 822 с.

14. Варфоломеев А. Методы криптографии и их применение в банковских технологиях: учебное пособие / А. Варфоломеев. М. Пеленицин. – М.: МИФИ, 1995. – 116 с.

15. Жельников В. Криптография от папируса до компьютера / В. Жельников. – М.: ABF, 1997 – 336 с.

16. Фомичев В. М. Симметричные криптосистемы: учебное пособие / В. М. Фомичев. – М. : МИФИ, 1995. – 325 с.

17. Давыдова Е. В. Новые средства криптографической защиты информации: учебное пособие / Е. В. Давыдова, И. Л. Дмитриев, И. А. Курепкин. – М. : МИФИ, 1996. – 132 с.

18. Гатчин Ю. А. Основы криптографических алгоритмов: учебное пособие / Ю. А. Гатчин, А. Г. Коробейников. – СПб.: СПбГИТМО (ТУ), 2002. – 29 с.

19. Голуб В. А. Парольная защита: учебно-методическое пособие / В. А. Голуб. – Воронеж: Изд-во ВГУ, 2005. – 15 с.

20. Васенин В. А. Информационная безопасность и компьютерный терроризм / В. А. Васенин // Сб. «Научные и методологические проблемы информационной безопасности». – М. : МЦНМО, 2004.

21. Актуальные проблемы анализа и синтеза сложных технических систем / ред. В. О. Никифоров // Научно-технический вестник СПбГУ ИТМО. – 2003. – Вып. 11. – 227 с.