Державний вищий навчальний заклад
«Ужгородський національний університет»
Факультет математики та цифрових технологій
Кафедра алгебри

“**ЗАТВЕРДЖУЮ**”
проректорів з наукової роботи

_____проф. Студеняк І.П.
“_____”_____20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Алгебраїчна теорія кодування і криптографія"

Рівень вищої освіти	**третій (освітньо-науковий)**
Галузь знань	**11 Математика і статистика**
Спеціальність	**111 Математика**
Освітня програма	**Математика**
Статус дисципліни	**Обов’язкова**
Мова навчання	**українська**

Ужгород – 2020 рік

Робоча програма навчальної дисципліни «Алгебраїчна теорія кодування і криптографія» для здобувачів третього (освітньо-наукового) рівня вищої освіти за спеціальністю 111 «Математика» галузі знань 11 «Математика і статистика».

Розробники: кандидат фіз.-мат. наук, доцент Тилищак О. А.

Робоча програма затверджена на засіданні кафедри алгебри

Протокол № ___ від. “__” _____ 2020 р.

Завідувач кафедрою канд. фіз.-мат. наук, доцент, Шапочка І. В.

_____ (_____)
(підпис) (прізвище та ініціали)

“_____”_____ 20___ р

1. Опис навчальної дисципліни:

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">денна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 6</td><td rowspan="2">Галузь знань
(шифр, назва)
11 «Математика і статистика»</td><td colspan="2" rowspan="2">Нормативна
(за вибором здобувача)</td></tr>
<tr></tr>
<tr><td rowspan="2">Модулів – 2</td><td rowspan="2">Напрям
111 «Математика»</td><td colspan="2" rowspan="2">Рік підготовки:</td></tr>
<tr></tr>
<tr><td>Змістових модулів – 12</td><td rowspan="4"></td><td>1-й</td><td></td></tr>
<tr><td></td><td>Семестр</td><td>Семестр</td></tr>
<tr><td>Загальна кількість годин –180</td><td>1-й</td><td>2-й</td></tr>
<tr><td rowspan="9"></td><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Освітньо-кваліфікаційний рівень:
Доктор філософії</td><td>12 год.</td><td>18 год.</td></tr>
<tr><td colspan="2">Практичні, лабораторні</td></tr>
<tr><td>12 год.</td><td>18 год.</td></tr>
<tr><td colspan="2">Семінарські</td></tr>
<tr><td colspan="2">Не передбачено</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>30 год.</td><td>30 год.</td></tr>
<tr><td>Вид контролю: залік</td><td>Вид контролю: іспит</td></tr>
</table>

Примітка.

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

для денної форми навчання — 60:120

2. Мета та завдання навчальної дисципліни

Основна мета курсу – ознайомити студентів з класичними поняттями, методами та досягненнями алгебраїчної теорії блокових кодів, що виправляють незалежні помилки, методами побудови і властивості кодів. Ознайомити з основними лінійними кодами: Хеммінга, БЧХ, Ріда-Маллера, Ріда-Соломона. Метод Бермана представлення кодів у вигляді ідеалів групових алгебр. Вивчення широко використовуваних криптографічних алгоритмів симетричного і асиметричного шифрування, а також криптографічних хеш-функцій.

Завдання – вміти застосовувати методи та результати сучасної алгебри для побудови кодів окремих видів, зясовувати їх властивості криптографії.

Загальні компетентності:

ЗК-1. Здатність до абстрактного мислення, аналізу та синтезу на основі логічних аргументів та перевірених фактів.

ЗК-5. Здатність демонструвати креативність у генеруванні нових ідей та досягненні наукових цілей

ЗК-8. Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.

Фахові компетентності:

ФК-1. Володіти найбільш передовими концептуальними та методологічними знаннями в галузі науково-дослідної та/або професійної діяльності і на межі предметних галузей і дослідницькими математичними методами та вміннями

ФК-3. Розроблення та реалізація проектів, включаючи власні дослідження в галузі математики, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику, і розв'язання проблем.

ФК-4. Здатність інтерпретувати результати досліджень, брати участь у семінарах, наукових конференціях, дискусіях із досвідченими науковцями-математиками стосовно наукового значення та потенційних наслідків отриманих результатів.

ФК-6. . Здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.

В результаті вивчення даного курсу студент повинен

- **знати:** основні результати алгебри і теорії чисел, розуміти проблеми складності алгоритмів;
- сучасні алгоритми кодування повідомлень і передачі даних по каналах зв'язку;
- коди Хемминга, циклічні коди, БЧХ, Ріда-Міллера, Ріда-Соломона;
- способи побудови кодів за елементами групових кілець;
- алгоритми симетричного і асиметричного шифрування, а також криптографічних хеш-функцій.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньо-наукової програми вивчення навчальної дисципліни «Алгебраїчна теорія кодування і криптографія» повинно забезпечити досягнення здобувачами третього рівня вищої освіти таких програмних результатів навчання (ПРН):

ПРН-2. Здобуття знань і розумінь поглибленого рівня у математиці та споріднених областях, включаючи методики проведення доведень і побудови математичних моделей, рівень цих знань повинен бути достатнім для проведення наукових досліджень на рівні останніх світових досягнень і направленим на їх розширення та поглиблення.

ПРН-9. Обізнаність та здатність взаємодіяти інтелектуально з найновішими математичними дослідженнями в спеціальній області дослідження.

ПРН-10. Досягнення відповідних знань, розумінь та здатностей використання методів аналізу даних і статистики на найсучаснішому рівні.

ПРН-11. Здатність створювати крупні програмні продукти на різних мовах програмування відповідно до потреб дисертаційного дослідження, а також адаптувати, удосконалювати та вбудовувати програмні продукти, початково призначені для іншої мети.

ПРН-12. Здатність планувати оригінальний вклад на основі дослідження до математичних знань, пов'язаних з важливою задачею, який є відповідної якості для друку.

ПРН-14. Здатність підготувати та успішно захистити дисертаційну роботу на основі індивідуальних досліджень, а також використати (та визнати) результати інших членів наукової групи.

Очікувані результати навчання (ПРН-2, ПРН-9, ПРН-10, ПРН-11, ПРН-12, ПРН-14):

- застосовувати результати алгебри і теорії чисел, для побудови кодів і оцінки їх параметрів;
- реалізовувати сучасні алгоритми кодування повідомлень і передачі даних по каналах зв'язку;
- коди Хемминга, циклічні коди, БЧХ, Ріда-Міллера, Ріда-Соломона;
- будувати коди заданих параметрів за елементами групових кілець;
- реалізовувати алгоритми симетричного і асиметричного шифрування, а також криптографічних хеш-функцій.

4. Засоби діагностики та критерії оцінювання результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- поточний контроль успішності,
- модульний контроль,
- підсумковий контроль.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю:

- вибіркове усне опитування перед початком занять;

- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- оцінювання якості та повноти виконання завдань модульної контрольної роботи.

Оцінювання знань здобувача здійснюється за 100-бальною шкалою (для екзаменів і заліків).

- максимальна кількість балів при оцінюванні знань студентів з дисципліни, яка завершується заліком , становить за успішність 100 балів;
- при оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань студентів за різними системами.

Шкала оцінювання: вузу, національна та ECTS

Оцінка ECTS	***Оцінка в балах***	***Оцінка за національною шкалою***		
		для екзамену, диференційованого заліку курсового проекту(роботи)		***для заліку***
A	90 – 100	5	***Відмінно***	***Зараховано***
B	82-89	4	***Добре***	
C	74-81			
D	64-73	3	***Задовільно***	
E	60-63			
FX	35-59	2	***Незадовільно*** *з можливістю повторного складання*	***Не зараховано*** *з можливістю повторного складання*
F	1-34	1	***Незадовільно*** *з обов'язковим повторним вивченням дисципліни*	***Не зараховано*** *з обов'язковим повторним вивченням дисципліни*

Критерій оцінювання з дисципліни

— "відмінно" A (90 та вище балів) заслуговує здобувач, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії;

— **"добре" B** (82-89 балів) заслуговує здобувач, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності;

— **"добре" C** (74-81 балів) заслуговує здобувач, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності;

— **"задовільно" D** (64-73 балів) заслуговує здобувач, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка “задовільно” виставляється здобувачам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;
— **"задовільно" E** (60-63 балів) заслуговує здобувач, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка “достатньо" виставляється здобувачам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача.
— **"незадовільно" FX** (35-59 балів) з можливістю повторного складання виставляється здобувачу, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.
— **"незадовільно" F** (1-34 балів) з обов’язковим повторним вивченням дисцтпліни виставляється здобувачу коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.

При виставленні оцінки можуть враховуватися результати навчальної роботи здобувача протягом семестру.

Іспит виставляється (без складання) у випадку набору кількості балів, що відповідає мінімальній оцінці "достатньо" (E).

Протягом семестру проводиться не менше двох модулів або колоквіумів чи контрольних робіт або інших видів контролю. Максимальна кількість балів, яка встановлюється для цих видів контролю, а також відповідність оцінок FX та F у шкалі ECTS, у балах та національній шкалі визначається Вченими радами факультетів або кафедрами, які забезпечують викладання відповідних дисциплін.

Розподіл балів, що присвоюється студентам

Поточне тестування та самостійна робота					Підсумковий тест (екзамен)	Сума
Семестри	Модуль 1	Практичні заняття	Інд. Р	СР	екзамен	100
1,2	50	30	-	20		

5. Програма навчальної дисципліни

Експоненціальна та поліноміальна складність алгоритмів. О-нотація. Кільце, група, поле Галуа, фробеніусове кільце, кільце класів лишків. Мультиплікативна група кільця класів лишків. Найбільший спільний дільник. Розширений алгоритм Евкліда. Функція Ейлера. Теорема Ейлера. Китайська теорема про залишки. Двійковий код. Відстань Хеммінга. Мінімальна відстань коду. Лінійний код. Породжуюча і перевірочна матриці лінійного коду. Код Хеммінга і його властивості. Визначення циклічного коду, властивості.

Архітектура кодера і декодера для цілического коду. Код Боуза-Чоудхурі-хоквінгема. Мажоритарне декодування лінійних кодів. Коди Ріда-Маллера, їх властивості. Недвійковий циклічні коди. Код Ріда-Соломона, його властивості.

Шифр зсуву. Шифр заміни. Шифр Віженера. Перестановочні шифри. Одноразовий шифр-блокнот. Алгоритм шифрування AES. Алгоритм шифрування 3DES. Алгоритм шифрування RC4. Завдання факторизации. Завдання дискретного логарифмування. Протокол широкоротої жаби. Протокол Нідхейма-Шредера. Протокол Отвей-Ріса. Алгоритм шифрування RSA. Ефективна реалізація розшифрування RSA. Атака на RSA: розділений модуль. Атака на RSA: мала шифрующая експонента. Атака на RSA: метод факторизації Ферма. Схеми поділ секрету. Алгоритм DSA. Підпис Шнорра. Підпис Ніберг-Руппель. Протокол електронного голосування.

Структура навчальної дисципліни

І семестр

	Денна форма					
	Усього	у тому числі				
		Л	п	лаб	інд	Ср
Теми	2	3	4	5	6	7
Відомості з теорії чисел, алгебраїчні структури, скінченні поля. Скінченні фробеніусові кільця.		4				8
Лінійні блокові коди, код Хеммінга, циклічні коди, БЧХ, Ріда-Міллера, Ріда-Соломона, Голея.		6	6			24
Побудова кодів за елементами групових кілець.		2	6			16
Усього годин		**12**	**12**			**48**

ІІ семестр

	Денна форма					
	Усього	у тому числі				
		Л	п	лаб	інд	Ср
Теми	2	3	4	5	6	7
Симетричне шифрування: докомп'ютерні шифри.		4	4			16
Огляд результатів К. Шеннона. Симетричне шифрування: огляд сучасних шифрів.		4	5			18
Асиметричне шифрування: односторонні функції і нові завдання криптографії.		4	5			18
Система шифрування RSA. Протоколи перевірки автентичності, протоколи розподілу секрету, протоколи цифрового підпису		8	4			24

Усього годин		**18**	**18**			**72**

Теми практичних занять

І семестр

№ з/п	Назва теми	Кількість Годин
1	Циклічні коди. Апаратна реалізація кодування і декодування. Коди БЧХ і Ріда-Міллера.	6
2	Недвійкові коди і коди Ріда-Соломона, Голея.	6
	Усього годин	12

ІІ семестр

№ з/п	Назва теми	Кількість Годин
3	Сучасні шифри симетричного шифрування.	4
4	Властивості розв'язку задачі параболічного типу з випадковими початковими умовами з простору Орліча.	5
5	Система шифрування RSA, протоколи перевірки автентичності, протоколи розподілу секрету, протоколи цифрового підпису.	5
6	Протокол електронного голосування.	4
	Усього годин	18

Самостійна робота

Визначення циклічного коду, властивості. Архітектура кодера і декодера для цілического коду. Код Боуза-Чоудхурі-хоквінгема. Мажоритарне декодування лінійних кодів. Недвійковий циклічні коди. Одноразовий шифр-блокнот. Алгоритм шифрування AES. Алгоритм шифрування 3DES. Алгоритм шифрування RC4. Завдання факторизации. Протокол широкоротої жаби. Протокол Нідхейма-Шредера. Протокол Отвей-Ріса. Алгоритм шифрування RSA. Атака на RSA: розділений модуль. Атака на RSA: мала шифрующая експонента. Атака на RSA: метод факторизації Ферма. Схеми поділу секрету. Алгоритм DSA. Підпис Шнорра. Підпис Ніберг-Руппель.

6. Рекомендована література

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Юрай Громкович; Пер. с нем.; Под ред. Б. Ф. Мельникова.?Издание 3-е.?Санкт-Петербург: БХВ-Петербург, 2010.?336 с.

2. Латыпов Р.Х. Электронный образовательный ресурс "Кодирование информации и криптография - Математические основы", 2012 http://zilant.kpfu.ru/course/view.php?id=3
3. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - - М.: Физматлит, 2012. - 280 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5300
4. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. URL: http://znanium.com/bookread.php?book=441493 5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://znanium.com/bookread.php?book=420047 7.2.

Додаткова література

1. Мальцев, Ю. Н. Элементы дискретной математики: элементы комбинаторики, теории графов теории кодирования и криптографии / Ю.Н. Мальцев, Е.П. Петров; М-во образования и науки РФ, Алт. гос. ун-т.?Барнаул: Изд-во Алт. гос. ун-та, 2004.?174 с
2. Латыпов, Р. Х. Математические основы кодирования информации и криптографии: учеб. пособие / Р. Х. Латыпов; Казан. гос. ун-т.?Казань: [КГУ], 2005.?59 с
3. Земор, Жиль. Курс криптографии / Жиль Земор; пер. с фр. В.В. Шуликовской.?Москва; Ижевск: Ин-т компьютер. исслед.: Регуляр. и хаотич. динамика, 2006.?255 с. 7.3.