**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Східноєвропейський національний університет імені Лесі Українки**
Кафедра прикладної математики та інформатики

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної і
навчальної роботи та рекрутації
проф. Гаврилюк С.В. _____
**Протокол №** 6 **від** 21.03. 2018 р.

# ПРИКЛАДНА ДИСКРЕТНА МАТЕМАТИКА

**ПРОГРАМА**
**нормативної навчальної дисципліни**
**підготовки магістра**
**спеціальності 014 Середня освіта**
**освітньої програми Інформатика**
**спеціальності 122 Комп'ютерні науки та інформаційні технології**
**освітньої програми Комп'ютерні науки та інформаційні технології**

Луцьк – 2018

**Програма навчальної дисципліни "Прикладна дискретна математика"** підготовки магістра галузі знань 01 Освіта, спеціальності 014 Середня освіта, за освітньою програмою Інформатика та галузі знань 12 Інформаційні технології спеціальності 122 Комп'ютерні науки та інформаційні технології за освітньою програмою Комп'ютерні науки та інформаційні технології.

12 січня 2018 р. – 11 с.

**Розробник** – доцент кафедри прикладної математики та інформатики,
канд. пед. наук Собчук О. М.

**Рецензент:** завідувач кафедри прикладної математики та інформатики,
д. ф.-м. наук, доц. Михайлюк В.О.

**Програма навчальної дисципліни затверджена на засіданні кафедри прикладної математики та інформатики**
протокол № 7 від 16.01.2018 р.

Завідувач кафедри _____ проф. Михайлюк В.О.

Програма навчальної дисципліни схвалена науково-методичною комісією факультету інформаційних систем, фізики та математики
протокол № 6 від 19.01.2018 р.

Голова науково-методичної
комісії факультету _____ доц. Полетило С.А.

Робоча програма навчальної дисципліни схвалена науково-методичною радою **Східноєвропейського національного університету імені Лесі Українки**

© Собчук О. М., 2018

## 1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| **Найменування показників** | **Галузь знань, спеціальність, освітня програма, освітній ступінь** | **Характеристика навчальної дисципліни** |
|---|---|---|
| Денна форма навчання | 12 Інформаційні технології<br>122 Комп'ютерні науки та інформаційні технології<br>Комп'ютерні науки та інформаційні технології<br><br>01 Освіта<br>014 Середня освіта (Інформатика)<br>Середня освіта (Інформатика)<br><br>магістр | нормативна |
| | | Рік навчання 5 |
| Кількість годин/кредитів 150/5 | | Семестр 9-ий |
| | | Лекції 24 год. |
| | | Практичні 28 год. |
| | | Самостійна робота 88 год. |
| ІНДЗ: немає | | Консультації 10 год. |
| | | Форма контролю: екзамен |

| **Найменування показників** | **Галузь знань, спеціальність, освітня програма, освітній ступінь** | **Характеристика навчальної дисципліни** |
|---|---|---|
| Заочна форма навчання | 01 Освіта<br>014 Середня освіта (Інформатика)<br>Середня освіта (Інформатика)<br><br>магістр | нормативна |
| | | Рік навчання 6 |
| Кількість годин/кредитів 150/5 | | Семестр 11-ий |
| | | Лекції 10 год. |
| | | Практичні 10 год. |
| | | Самостійна робота 112 год. |
| ІНДЗ: немає | | Консультації 18 год. |
| | | Форма контролю: екзамен |

## 2. АНОТАЦІЯ КУРСУ:

**Вступ**

Нормативна навчальна дисципліна "Прикладна дискретна математика" є складовою циклу навчальних дисциплін загальної підготовки фахівців освітнього ступеня магістр. Предметом вивчення навчальної дисципліни є сучасні дослідження у галузі прикладної дискретної математики. Попередні знання з дисциплін: дискретна математика, маематична логіка, алгебра і теорія чисел, методи обчислень, паралельні та розподілені обчислення, основи комп'ютерної

безпеки, інтелектуаьні системи, теорія складності обчислень, системи і методи прийняття рішень, моделювання економічних, екологічних та соціальних процесів та ін.

Предметом вивчення навчальної дисципліни є сучасні дослідження у галузі прикладної дискретної математики. Основними завданнями є ознайомити студентів з сучасними науковии дослідженнями в галузі прикладної дискретної математики, систематизувати знання з базових навчальних дисциплін, формувати вміння і навички аналізу джерел наукової інформації.

## 3. КОМПЕТЕНЦІЇ

До кінця навчання студенти будуть компетентними у таких питаннях:

*Магістр повинен знати*: алгебраїчні структури, дискретні функції, комбінаторний аналіз; методи криптоаналізу, криптографічні протоколи; математичні основи комп'ютерної безпеки; математичні моделі і методи аналізу, синтезу, оптимізації та оцінки складності дискретних автоматів; математичні основи інтелектуальних систем.

*Магістр повинні вміти*: розв'язувати системи рівнянь над скінченими полями і кільцями; здійснювати оцінку стійкості криптосистем, застосовувати математичні методи аналізу функціональної стійкості обчислювальних і керуючих систем; застосовувати методи аналізу, синтезу, оптимізації та оцінки складності дискретних автоматів; будувати дискретні моделі реальних процесів – у фізиці, економіці, біології та ін.

## 4. . ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

На вивчення навчальної дисципліни відводиться 150 годин / 5 кредитів.

Навчальна дисципліна складається з таких **змістових модулів**:

1. Теоретичні основи прикладної дискретної математики
2. Математичні методи захисту інформації
3. Прикладна теорія автоматів

**Структура навчальної дисципліни для денної форми навчання**

| Назви змістових модулів і тем | Кількість годин | | | | |
|---|---|---|---|---|---|
| | Усього | у тому числі | | | |
| | | Лек. | Практ. роб. | Сам. роб. | Конс. |
| **Змістовий модуль 1. Теоретичні основи прикладної дискретної математики** | | | | | |
| Тема 1. Теоретичні основи прикладної дискретної математики. | 6 | 2 | | 4 | |
| Тема 2. Прикладна теорія графів | 6 | 2 | 2 | 2 | |
| Тема 3. Прикладна теорія кодування | 8 | 2 | 2 | 4 | |
| Тема 4. Математичні основи інформатики та програмування. | 6 | 2 | 2 | 2 | |
| Тема 5. Обчислювальні методи в дискретній математиці | 8 | 2 | 2 | 4 | |
| Тема 6. Математичні основи інтелектуальних систем | 8 | 2 | 2 | 2 | 2 |
| Тема 7. Історичні нариси з дискретної математики та її застосувань | 10 | | | 10 | |

| | | | | | |
|---|---|---|---|---|---|
| Разом за змістовим модулем 1 | 52 | 12 | 10 | 28 | 2 |
| **Змістовий модуль 2. Математичні методи захисту інформації** | | | | | |
| Тема 8. Математичні методи криптографії | 16 | **2** | **2** | **12** | |
| Тема 9. Математичні основи комп'ютерної безпеки | 18 | **2** | **2** | **12** | **2** |
| Тема 10. Математичні основи надійності обчислювальних і керуючих систем (ОіКС) | 16 | 2 | 4 | 8 | 2 |
| Разом за змістовим модулем 2 | 50 | 6 | 8 | 32 | 4 |
| **Змістовий модуль 3. Прикладна теорія автоматів** | | | | | |
| Тема 11. Прикладна теорія автоматів | 16 | 2 | 2 | 10 | 2 |
| Тема 12. Логічне проектування дискретних автоматів | 14 | 2 | 4 | 8 | |
| Тема 13. Дискретні моделі реальних процесів | 18 | 2 | 4 | 10 | 2 |
| Разом за змістовим модулем 3 | 48 | 6 | 10 | 28 | 4 |
| **Всього годин** | **150** | **24** | **28** | **88** | **10** |

**Структура навчальної дисципліни для заочної форми навчання**

| **Назви змістових модулів і тем** | **Кількість годин** | | | | |
|---|---|---|---|---|---|
| | **Усього** | **у тому числі** | | | |
| | | **Лек.** | **Практ. роб.** | **Сам. роб.** | **Конс.** |
| **Змістовий модуль 1. Теоретичні основи прикладної дискретної математики** | | | | | |
| Тема 1. Теоретичні основи прикладної дискретної математики. | 4 | | | 4 | |
| Тема 2. Прикладна теорія графів | 8 | 1 | 1 | 6 | |
| Тема 3. Прикладна теорія кодування | 8 | 1 | 1 | 6 | |
| Тема 4. Математичні основи інформатики та програмування. | 9 | 1 | | 6 | 2 |
| Тема 5. Обчислювальні методи в дискретній математиці | 8 | 1 | 1 | 6 | |
| Тема 6. Математичні основи інтелектуальних систем | 10 | 1 | 1 | 6 | 2 |
| Тема 7. Історичні нариси з дискретної математики та її застосувань | 12 | | | 10 | 2 |
| Разом за змістовим модулем 1 | 59 | 5 | 4 | 44 | 6 |
| **Змістовий модуль 2. Математичні методи захисту інформації** | | | | | |
| Тема 8. Математичні методи криптографії | 16 | **1** | **1** | **12** | **2** |
| Тема 9. Математичні основи комп'ютерної безпеки | 16 | **1** | **1** | **12** | **2** |
| Тема 10. Математичні основи надійності обчислювальних і керуючих систем (ОіКС) | 17 | 1 | 2 | 12 | 2 |
| Разом за змістовим модулем 2 | 49 | 3 | 4 | 36 | 6 |
| **Змістовий модуль 3. Прикладна теорія автоматів** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Тема 11. Прикладна теорія автоматів | 14 | 1 | 1 | 10 | 2 |
| Тема 12. Логічне проектування дискретних автоматів | 16 | 1 | 1 | 12 | 2 |
| Тема 13. Дискретні моделі реальних процесів | 12 | | | 10 | 2 |
| Разом за змістовим модулем 3 | 42 | 2 | 2 | 32 | 6 |
| **Всього годин** | **150** | **10** | **10** | **112** | **18** |

## 5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

1. *Опрацювання теоретичних основ лекційного матеріалу.*
2. *Самостійне опрацювання матеріалу з тем:*

**Змістовий модуль 1. Теоретичні основи прикладної дискретної математики**

Алгебраїчні структури, дискретні функції, комбінаторний аналіз, теорія чисел, математична логіка, теорія інформації, системи рівнянь над скінченими полями і кільцями;

Графові моделі в інформатиці та програмуванні, в комп'ютерній безпеці, обчислювальних і керуючих системах, в інтелектуальних системах.

Коди для стиснення даних та захисту інформації, коди для виявлення та виправлення помилок, побудова оптимальних кодів, аналіз властивостей кодів;

Формальні мови та граматики, алгоритмічні системи, мови програмування, структури і алгоритми обробки даних, теорія обчислювальної складності;

Теоретико-числові методи в криптографії, обчислювальні методи в теорії чисел і загальної алгебрі, комбінаторні алгоритми, паралельні обчислення, методи дискретної оптимізації;

Бази даних, бази знань, логічний висновок, експертні системи, математична лінгвістика, формалізація природних мов, аналіз текстів;

Історичні нариси з дискретної математики та її застосувань в криптографії, комп'ютерній безпеці, кібернетиці, інформатиці, програмуванні та теорії надійності.

**Змістовий модуль 2. Математичні методи захисту інформації**

Синтез криптосистем, методи криптоаналізу, генератори псевдовипадкових послідовностей, оцінка стійкості криптосистем, криптографічні протоколи, математичні методи квантової криптографії;математичні методи стеганографії - синтез стеганосистем, методи стеганоаналізу, оцінка стійкості стеганосистем;

Математичні моделі безпеки комп'ютерних систем (КС), математичні методи аналізу безпеки КС, математичні методи синтезу захищених КС;

Математичні моделі функціональної стійкості ОіКС (до відмов, несправностей, збоїв, змагань, дослідження), математичні методи аналізу функціональної стійкості ОіКС, математичні методи синтезу функціонально стійких ОіКС, математичні методи верифікації логічних схем і програм, математичні методи синтезу схем здатних до самоперевірки та контролю;

**Змістовий модуль 3. Прикладна теорія автоматів**

Автоматні моделі мережевих протоколів, криптосистем і керуючих систем, автомати без втрати інформації, експерименти з автоматами, декомпозиція автоматів, автоматні рівняння, клітинні автомати;

Математичні моделі і методи аналізу, синтезу, оптимізації та оцінки складності дискретних автоматів, апаратна реалізація криптоалгоритмів;

Математичне моделювання реальних процесіву фізиці, економіці, біології та ін. (дискретно-подієве, клітинно-автоматне і т.п. моделювання).

## 6. ВИДИ (ФОРМИ) ІНДИВІДУАЛЬНИХ НАУКОВО-ДОСЛІДНИХ ЗАВДАНЬ (ІНДЗ)

ІНДЗ з кожного модуля передбачає підготовку реферативного повідомлення з виступом на практичному занятті за тематикою наукових статей журналу «Прикладная дискретная математика» // http://www.mathnet.ru/php/archive.phtml?jrnid=pdm&wshow=contents&option_lang=rus

## 7. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Оцінювання знань і умінь студентів здійснюється за модульно-рейтинговою системою. Максимальна кількість балів, яку студент може отримати протягом усього вивчення курсу, становить 100.

Підсумкова оцінка за 100-бальою шкалою складається із сумарної кількості балів за:

- поточне оцінювання з відповідних тем (максимум 15 балів);
- самостійне опрацювання теоретичного матеріалу з тем, які зараховуються у поточний контроль (максимум 25 балів);
- модульний контроль (максимум 60 балів).

| **Поточний контроль** | | | | **Модульний контроль** | | | **Загальна кількість балів** |
|---|---|---|---|---|---|---|---|
| **(max = 40 балів)** | | | | **(max = 60 балів)** | | | |
| **Модуль1** | | | **Модуль2** | **Модуль3** | | | |
| **ПРАКТИЧНІ ЗАНЯТТЯ** | | | **САМОСТІЙНА РОБОТА** | **ІНДИВІДУАЛЬНІ ЗАВДАННЯ** | | | |
| **ЗМ 1** | **ЗМ 2** | **ЗМ 3** | **25** | **ЗМ 1** | **ЗМ 2** | **ЗМ 3** | **100** |
| **5** | **5** | **5** | | **20** | **20** | **20** | |

Під час поточного контролю на практичних заняттях оцінюється виконання студентом завдань кожного заняття (максимальна оцінка 5 балів за кожне заняття) та виводиться середнє значення в межах змістового модуля. Оцінюється якість підготовки до занять, наявність конспектів, участь у дискусії, доповнення.

Модульний контроль проводиться у формі захисту наукових повідомлень відповідно до індивідуальних завдань за змістовими модулями I, II та III.

Оцінюється: складність, науковість, актуальність, системність і повнота у розкритті теми (10 балів), аргументованість висновків (5 балів), грамотність викладу та культура оформлення (5 балів).

**Шкала оцінювання:**

| **Оцінка в балах за всі види навчальної діяльності** | **Оцінка** | |
|---|---|---|
| | **для екзамену** | **для заліку** |
| 90-100 | Відмінно | Зараховано |
| 82-89 | Дуже добре | |
| 75-81 | Добре | |
| 68-74 | Задовільно | |
| 67-60 | Достатньо | |
| 0-59 | Незадовльно | Незараховано (з можливістю повторного складання) |

## 8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Айзенберг Н.Н. Многозначная пороговая логика. / Айзенберг Н.Н. , Иваськив Ю.Л. – К.: Наукова думка, 1977.

2. Бакнелл Д. М. Фундаментальные алгоритмы и структуры данных в Delphi / Бакнелл Д. М. – СПб.: DiaSoft, 2003.

3. Бенькович Е. С. Практическое моделирование динамических систем /Бенькович Е. С., Колесов Ю. Б., Сениченков Ю. Б. – СПб.: БВХ-Петербург, 2002.

4. Бережная Е. В. Математические методы моделирования экономических систем / Бережная Е. В., Бережной В. И. – М.: Финансы и статистка, 2002.

5. Бондаренко МФ. Комп’ютерна дискретна математика / Бондаренко МФ., Білоус Н.В., Руткас А.Г. – Х.: Компанія СМІТ, 2004

6. Галицкий А.В. Защита информации в сети- анализ технологий и синтез решений / Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. – М.: ДМК Пресс, 2004.

7. Гильбетр Д. Основания математики: Логические исчисления и формализация арифметики. Пер. с нем. 2-е изд / Гильбетр Д., Бернайс.М.:Наука, 1982.

8. Глибовець М. М. Основи комп'ютерних алгоритмів / Глибовець М. М. – К.: КМ Академія, 2003.

9. Глоба Л.С. Концептуальное проектирование информационно-аналитических систем для сложных административных структур стратегического уровня управления / Глоба Л.С., Голышев Л.К., Терновой М.Ю. – К.: Інформ.-аналіт. агенство, 2008.

10. Голиков А. П. Экономико-математическое моделирование мирохозяйственных процессов / Голиков А. П. – Х.: ХНУ им. В.Н. Каразина, 2003.

11. Грездов Г. Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы / Грездов Г. Г. – К.: ГУИКТ, 2009.

12. Гудрич М. Структуры данных и алгоритмы в Java / Гудрич М., Тамассия Р. – Минск: Новое знание, 2003.

13. Драгалин Д.Г. Математический интуиционизм. Введение в теорию доказательств / Драгалин Д.Г. – М.: Наука, 1979.

14. Єріна А.М. Статистичне моделювання та прогнозування: Навч. посіб. / Єріна А.М. – К.: КНЕУ, 2001.

15. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. – М.: КУДИЦ-ОБРАЗ, 2001. 4

16. Йордон Э. Структурные модели в объектно-ориентированном анализе и проектировании / Йордон Эдвард, Аргила Карл – М.: Лори, 1999.

17. Кейслер Г. Теория моделей / Кейслер Г., Чэн Ч. Ч. – М.: Мир, 1977.

18. Клакович Л. М. Теорія алгоритмів / Клакович Л. М., Левицька С. М., Костів О. В. – Львів: ЛНУ ім. І. Франка, 2008.

19. Кормен Т. Алгоритмы: построение и анализ / Кормен Т., Лейзерсон Ч., Ривест Р. – М.: МЦНМО, 2004.

20. Лыскова В. Логика в информатике / Лыскова В., Ракитина Е. М.: Лаборатория Базовых Знаний, 2001.

21. Лянце В. Вступ до нестандартної теорії ймовірностей / Лянце В., Чуйко Г. – Львів : Видавн. центр ЛНУ ім. І. Франка, 2002.

22. Матвійчук А. В. Аналіз та прогнозування розвитку фінансово-економічних систем із використанням теорії нечіткої логіки / Матвійчук А. В. – К.: Центр навч. л-ри, 2005.

23. Машина Н. І. Вищі фінансові обчислення / Машина Н. І. – К.: Центр навч. л-ри, 2003.

24. Медведєв М. Г. Ігрові методи моделювання економічних систем / Медведєв М. Г., Барановська Л. В. – К.: Вид-во Європ. ун-ту, 2002.

25. Менаске Д. А. Производительность Web-служб: Анализ, оценка и планирование / Менаске Д. А., Алмейда В. А. – М.: DiaSoft, 2003. 5

26. Непейвода Н. Н. Прикладная логика / Непейвода Н. Н. Новосибирск: Изд-во Новосиб. ун-та, 2000.

27. Пономаренко Л.А. Основи економічної кібернетики / Пономаренко Л.А. – К.: Київ. нац. торг.-екон. ун-т, 2002.

28. Прокопов С. В. Экономико-математическое моделирование промышленного производства / Прокопов С. В. – К.: Ин-т экономики НАН Украины., 2003.

29. Рогальский Ф. Б. Математические методы анализа экономических систем. В 2 кн. / Рогальский Ф. Б., Курилович Я. Е., Цокуренко А. А. – К.: Наук. думка, 2001.

30. Седжвик Р. Фундаментальные алгоритмы на Java. Ч. 1-4. Анализ. Структуры данных. Сортировка. Поиск. Седжвик Роберт К. [и др.] – М. : DiaSoft, 2003.

31. Седжвик Р. Фундаментальные алгоритмы на С++: Анализ, структуры данных, сортировка, поиск: Ч. 1-4 / Седжвик Р. К. [и др.]– М. : DiaSoft, 2001.

32. Трохимчук П. П. Теорія виведення в нестандартних логіках / Трохимчук П. П. – Луцьк: Вежа, 2004.

33. Ховард М. Защищенный код / Ховард Майкл, Лебланк Дэвид – М.: Рус. Ред., 2004.

34. Хорошко В. А. Методы и средства защиты информации / Хорошко В. А., Чекатков А. А. К.: Юниор, 2003.

35. Юхимчук С. В. Математичні моделі ризику для систем підтримки прийняття рішень / Юхимчук С. В., Азарова А. О. – Вінниця: Універсум., 2003.

36. Янковой О. Г. Моделювання парних зв'язків в економіці / Янковой О. Г. – О.: Оптимум, 2001.

## 9. ПЕРЕЛІК ПИТАНЬ ДО ЕКЗАМЕНУ

1. Алгебраїчні структури.
2. дискретні функції.
3. системи рівнянь над скінченими полями і кільцями.
4. Графові моделі в інформатиці та програмуванні.
5. Графові моделі в комп'ютерній безпеці.
6. Графові моделі в обчислювальних системах.
7. Графові моделі в керуючих системах.
8. Графові моделі в інтелектуальних системах.
9. Коди для стиснення даних
10. Коди для захисту інформації.
11. Коди для виявлення
12. Коди для виправлення помилок
13. Побудова оптимальних кодів
14. Аналіз властивостей кодів.
15. Формальні мови та граматики.
16. Алгоритмічні системи.
17. Теорія обчислювальної складності.
18. Теоретико-числові методи в криптографії.
19. Обчислювальні методи в теорії чисел.
20. Методи дискретної оптимізації;
21. Експертні системи
22. Формалізація природних мов.
23. Аналіз текстів;
24. Синтез криптосистем.
25. Методи криптоаналізу.
26. Генератори псевдовипадкових послідовностей.
27. Оцінка стійкості криптосистем.
28. Математичні методи квантової криптографії.
29. Математичні методи стеганографії.
30. Синтез стеганосистем.
31. Методи стеганоаналізу
32. Оцінка стійкості стеганосистем;
33. Математичні моделі безпеки комп'ютерних систем (КС).
34. Математичні методи аналізу безпеки КС.
35. Математичні методи синтезу захищених КС.
36. Математичні моделі функціональної стійкості ОіКС.
37. Мематичні методи аналізу функціональної стійкості ОіКС.
38. Математичні методи синтезу функціонально стійких ОіКС.
39. Математичні методи верифікації логічних схем і програм.

40. Математичні методи синтезу схем здатних до самоперевірки та контролю.
41. Автоматні моделі мережевих протоколів, криптосистем і керуючих систем.
42. Автомати без втрати інформації. Декомпозиція автоматів.
43. Автоматні рівняння.
44. Клітинні автомати
45. Математичні моделі дискретних автоматів.
46. Методи аналізу дискретних автоматів.
47. Математичні методи синтезу дискретних автоматів.
48. Математичні методи оптимізації дискретних автоматів.
49. Математичні методи оцінки складності дискретних автоматів.
50. Апаратна реалізація криптоалгоритмів.
51. Математичне моделювання реальних процесів у фізиці
52. Математичне моделювання реальних процесів в економіці.
53. Математичне моделювання реальних процесів у біології .