



КОМБІНАТОРНИЙ АНАЛІЗ. ЧАСТИНА 2 (ПО 2.2)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Обов'язкова (нормативна) (цикл загальної підготовки)</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>2 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 4.5 кредитів ЄКТС / 135 годин Лекційних занять: 36 годин Практичних занять: 36 годин Самостійна робота студентів: 63 години</i>
Семестровий контроль/ контрольні заходи	<i>екзамен, МКР, РР</i>
Розклад занять	http://rozklad.kpi.ua http://ipt.kpi.ua/navchalnij-protses
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: проф. Савчук Михайло Миколайович (mikhail.savchuk@gmail.com) Практичні: доц. Яковлев Сергій Володимирович, (vasv@rl.kiev.ua) ас. Оксьоненко Максим Петрович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Різні розділи комбінаторного аналізу включаються як складова частина або застосовуються у багатьох математичних дисциплінах, наприклад таких, як дискретна математика, алгебра математичний аналіз, теорія ймовірностей, теорія інформації та кодування, теорія булевих функцій, криптологія та ін. Для підготовки фахівців за спеціальністю «Прикладна математика» необхідне цілісне послідовне виконання основних задач та методів комбінаторного аналізу. Знання основних понять комбінаторики, володіння методами комбінаторного аналізу вкрай необхідно фахівцям, що займаються математичними методами захисту інформації, створенням систем криптографічного захисту інформації та їх аналізом. Дисципліна знайомить студентів з класичними задачами та методами комбінаторики, а також з сучасними комбінаторними методами, що застосовуються в криптографії та криптоаналізі.

Метою кредитного модуля «Комбінаторний аналіз 1» є надання студентам знання в галузі комбінаторної математики та поєднання їх із іншими розділами фундаментальної та прикладної математики (математичного аналізу, лінійної та прикладної алгебри). Зокрема, розглядаються поняття дискретних ймовірностей та дискретних випадкових величин, методи асимптотичного

оцінювання рядів та послідовностей, детальні алгоритми генерування комбінаторних об'єктів, абстрактні алгебраїчні методи аналізу комбінаторних конфігурацій. Завдання кредитного модуля – дати можливість студентам освоїти основні методи аналізу комбінаторних конфігурацій з заданими характеристиками, побудови комбінаторних алгоритмів (детермінованих та імовірнісних) та оцінки цих алгоритмів. Наводяться приклади застосування методів комбінаторики в алгебрі, теорії чисел, кодуванні, криптографії, теорії складності та теорії алгоритмів. Багато уваги приділяється дослідженню комбінаторних алгоритмів, загальним комбінаторним схемам, практичним застосуванням методів комбінаторного аналізу.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі компетентності та програмні результати навчання за освітньою програмою:

Загальні компетентності

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями

ЗК 3 – Здатність генерувати нові ідеї (креативність)

ЗК 4 – Здатність бути критичним і самокритичним

ЗК 6 – Здатність до абстрактного мислення, аналізу та синтезу

ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел

ЗК 8 – Знання та розуміння предметної області та розуміння професійної діяльності

Фахові компетентності

ФК 1 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем

ФК 2 – Здатність виконувати завдання, сформульовані у математичній формі

ФК 13 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних

ФК 14 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних

ФК 18 – Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем

Програмні результати навчання

РН 1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці

РН 3 – Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів.

РН 4 – Виконувати математичний опис, аналіз та синтез дискретних об'єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів

РН 7 – Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач

РН 9 – Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних ресурсів алгоритми для чисельного дослідження математичних моделей та розв'язання практичних задач.

РН 14 – Виявляти здатність до самонавчання та продовження професійного розвитку.

РН 15 – Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу

РН 19 – Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

РН 21 – Вміти формулювати та розв'язувати алгебраїчні та комбінаторні задачі, будувати та реалізовувати комбінаторні алгоритми та алгоритми прикладної алгебри, аналізувати теоретичну та практичну складність таких алгоритмів

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для засвоєння матеріалу курсу «Комбінаторний аналіз» студент повинен опанувати курс «Дискретна математика» та вільно орієнтуватись в матеріалах курсів «Математичний аналіз» та «Алгебра та геометрія», які вивчаються паралельно.

Отримані практичні навички та засвоєнні знання необхідні для опанування таких дисциплін як «Спеціальні розділи обчислювальної математики», «Симетрична криптографія», «Асиметричні криптосистеми та протоколи», «Теорія інформації та кодування».

3. Зміст навчальної дисципліни

Розділ 1. Класична теорія ймовірностей

Тема 1.1. Класична теорія ймовірностей. Випадкові величини. Ймовірнісний розподіл.

Функції від випадкових величин.

Тема 1.2. Функція розподілу. Кількість випадкових величин з заданим розподілом. Сумісний розподіл випадкових величин. Незалежні випадкові величини.

Тема 1.3. Математичне сподівання, дисперсія і середнє квадратичне відхилення випадкової величини. Твірна функція випадкової величини.

Тема 1.4. Вироджені, двоточкові, бернуллівські випадкові величини і їх розподіли. Схема незалежних випробувань. Біноміальні випадкові величини і біноміальний розподіл.

Тема 1.5. Інші важливі дискретні розподіли і випадкові величини.

Розділ 2. Основні поняття математичної теорії інформації. Булеві функції. Ймовірності і ентропія на функціях і відображеннях.

Тема 2.1. Основні поняття математичної теорії інформації.

Тема 2.2. Булеві функції та способи їх зображення.

Тема 2.3. Випадкові булеві функції. Складність булевих функцій. Ймовірності і ентропія на функціях і відображеннях.

Розділ 3. Комбінаторні алгоритми. Лексикографічний порядок. Породження перестановок та підмножин в заданому порядку. Породження випадкових перестановок та підмножин.

Тема 3.1. Комбінаторні алгоритми. Лексикографічний порядок. Індекс перестановки.

Тема 3.2. Факторіальна система числення. Породження перестановок.

Тема 3.3. Породження всіх підмножин.

Тема 3.4. Породження підмножин потужності n -множини.

Тема 3.5. Породження випадкових перестановок і випадкових підмножин.

Розділ 4. Асимптотичний аналіз комбінаторних формул.

Тема 4.1. Базові асимптотичні поняття і співвідношення. Числа і многочлени Бернуллі. Формула Ойлера-Маклорена.

Тема 4.2. Асимптотика гармонічних чисел. Формула Стірлінга.

Розділ 5. Спеціальні матриці

Тема 5.1. Пряма сума і прямий добуток матриць. Матриці перестановки. Стохастичні матриці.

Тема 5.2. Матриці Адамара.

Розділ 6. Підстановки, групи підстановок. Загальна комбінаторна схема.

Тема 6.1. Підстановки. Симетрична група підстановок. Степені підстановки. Граф підстановки. Циклова структура. Порядок підстановки. Підгрупи симетричної групи.

Тема 6.2. Загальна комбінаторна схема.

4. Навчальні матеріали та ресурси

1. Кривий, Сергій Лук'янович. Дискретна математика : підручник для студентів вищих навчальних закладів / С.Л. Кривий ; Міністерство освіти і науки України, Київський національний університет імені Тараса Шевченка, Хмельницький національний університет. - Київ ; – Чернівці : Букрек, 2017. – 567 с.
2. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцький Г.М., Печурін М.К. Основи дискретної математики. – К.: Наукова думка, 2002. – 580 с.
3. Карнаух, Тетяна Олександрівна. Комбінаторика : навч. посіб. для студ. вищ. навч. закл., що навчаються за напрямом "Прикладна математика" / Т. О. Карнаух ; Київ. нац. ун-т ім. Тараса Шевченка. - Київ : Київський ун-т, 2011. - 143 с.
4. Дискретні структури (Алгебраїчні та числові системи, комбінаторний аналіз) : навчально-методичний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення», аспірантів та викладачів вищих навчальних закладів / Укладач : Бойко І.В., Петрик М.Р., Цуприк Г.Б. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 64 с.
5. Донець Г. П. Екстремальні задачі на комбінаторних конфігураціях : монографія / Г. П. Донець, Л. М. Колечкіна. – Полтава : РВВ ПУЕТ, 2011. – 309 с.
6. Гнеденко Б.В. Курс теорії ймовірностей. – К.: ВПЦ Київський університет, 2010. – 464 с.
7. Турчин В.Н. Теорія ймовірностей і математична статистика. Основні поняття, приклади, задачі: Підручник для студентів вищих навчальних закладів. – Дніпропетровськ: ІМА-прес, 2014. - 556 с.
8. Reincold E., Nievergelt J., Deo N. Combinatorial Algorithms. Theory and Practice. – New Jersey: Prentice-Hall, Inc., Englewood Cliffs, 1977.
9. Базилевич, Лідія Євгенівна. Дискретна математика у прикладах і задачах : підручник / Л.Є. Базилевич. – Львів : І.Е. Чижиков, 2013. – 486 с.
10. Кривий, Сергій Лук'янович. Збірник задач з дискретної математики : навчальний посібник для студентів вищих навчальних закладів / С.Л. Кривий ; Міністерство освіти і науки України, Київський національний університет імені Тараса Шевченка. – Київ ; – Чернівці : Букрек, 2018. – 455 с.

Для кращого опанування матеріалів дисципліни студентам надаються електронні конспекти лекцій та відеозаписи практичних занять

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються такі методи навчання: для лекційних занять – пояснювально-ілюстративний метод та метод проблемного викладу; для практичних занять – пояснювально-ілюстративний метод, репродуктивний метод та метод проблемного викладу. Захист розрахункової роботи передбачає використання дискусійного методу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
Розділ 1. Класична теорія ймовірностей	
1	Дискретні випадкові величини і ймовірнісні розподіли в класичній схемі ймовірностей. Функції від випадкової величини. Розподіл випадкової величини, яка є функцією від іншої випадкової величини. Теорема Колмогорова про побудову випадкової величини за законом розподілу в класичній схемі ймовірностей
2	Функція розподілу. Кількість випадкових величин з заданим розподілом в класичній схемі. Сумісний розподіл випадкових величин. Умови узгодженості для двох випадкових величин. Сумісний розподіл дискретних випадкових величин. Незалежні випадкові величини. Еквівалентність різних означень незалежності для дискретних випадкових величин
3	Математичне сподівання випадкової величини. Дисперсія та середнє квадратичне відхилення випадкової величини. Твірна функція (генератриса) випадкової величини. Обчислення ймовірностей розподілу, математичного сподівання і дисперсії за допомогою генератрис. Математичне сподівання суми. Математичне сподівання добутку двох незалежних випадкових величин. Дисперсія та генератриса суми незалежних випадкових величин
4	Вироджена випадкова величина. Двоточкові випадкові величини та їх розподіли. Математичне сподівання, дисперсія, генератриса цих випадкових величин. Незалежність двоточкових та індикаторних випадкових величин, зв'язок з відповідними подіями. Схема незалежних випробувань і незалежних випробувань Бернуллі. Біноміальні випадкові величини і біноміальний розподіл. Математичне сподівання, дисперсія, генератриса біноміальної випадкової величини
5	Інші базові дискретні випадкові величини і розподіли: геометричний розподіл, Пуассона, від'ємний біноміальний розподіл, гіпергеометричний. Означення, обчислення математичного сподівання, дисперсії, генератрис для цих випадкових величин. Граничні теореми
Розділ 2. Основні поняття математичної теорії інформації. Булеві функції. Ймовірності і ентропія на функціях і відображеннях.	
6	Основні поняття математичної теорії інформації. Ймовірнісний ансамбль і ентропія. Сукупна ентропія двох ймовірнісних ансамблів. Умовна ентропія. Взаємна інформація ансамблів X та Y . Ентропія на символ джерела
7	Булеві функції та способи їх зображення. Означення булевої функції. Таблиця істинності, досконала диз'юнктивна нормальна форма, поліном Жегалкина, ряд Фур'є. Кількість булевих функцій
8	Випадкові булеві функції. Складність булевих функцій. Випадкові булеві функції і складність їх реалізації. Ймовірності і ентропія на функціях і відображеннях. Приклади застосувань в криптографії
Розділ 3. Комбінаторні алгоритми. Лексикографічний порядок. Породження перестановок та підмножин в заданому порядку. Породження випадкових перестановок та підмножин	
9	Комбінаторні алгоритми. Лексикографічний порядок на декартовому добутку. Індекс перестановки. Алгоритм обчислення індексу перестановки. Лексикографічний порядок на множині перестановок. Факторіальна система числення. Породження перестановок. Алгоритми породження перестановок за індексом, в лексикографічному порядку, з мінімальними змінами
10	Породження всіх підмножин. Взаємно однозначні відповідності між булеаном, множиною всіх n -векторів і множиною характеристичних функцій. Лексикографічний порядок в двійковому представленні. Породження всіх підмножин n -множини в лексикографічному порядку двійкового представлення. Побудова n -розрядного двійково-віддзеркаленого коду Грея. Породження всіх підмножин n -множини з мінімальними змінами

11	Породження k -підмножин n -множини. Взаємно однозначна відповідність між множиною всіх підмножин потужності n -множини і всіх булевих n -векторів ваги k . Алгоритми породження всіх k -підмножин n -множини в лексикографічному порядку двійкового представлення. Лексикографічний порядок на k -підмножинах n -множини, індукований лексикографічним порядком на декартовому добутку. Алгоритми породження усіх k -підмножин n -множини в лексикографічному порядку.
12	Моделювання випадкових перестановок і підмножин. Датчики випадкових чисел. Породження випадкових перестановок: з випадковим вибором індексу, з використанням випадкових транспозицій, з розміщенням послідовно випадкових чисел або послідовним розміщенням чисел від 1 до n на випадкові позиції, рекурентно з випадковим переходом до перестановки на одиницю більшої потужності. Породження випадкових підмножин n -множини. Генерування випадкової k -підмножини n -множини: алгоритм з використанням випадкової перестановки та алгоритми з послідовним розміщенням одиниць
Розділ 4. Асимптотичний аналіз комбінаторних формул	
13	Асимптотичний аналіз. Порівняння функцій в околі граничної точки, символи Ландау. Приклади, базові асимптотичні співвідношення і означення. Ієрархія функцій. Числа і многочлени Бернуллі. Формула Ойлера-Маклорена
14	Доведення асимптотичної формули для гармонічних чисел з використанням формули Ойлера-Маклорена. Формула Стірлінга для $n!$
Розділ 5. Скінченно-різницеві оператори і комбінаторні числа	
15	Спеціальні матриці. Пряма сума і прямиий добуток матриць. Тотожності і співвідношення з використанням операцій суми, добутку, прямої суми, прямого добутку, транспозиції матриць. Матриці перестановки, ортогональність рядків (стовпців), операції з матрицями, інші властивості
16	Стохастичні і двічі стохастичні матриці, операції, інші властивості. Представлення двічі стохастичної матриці як випуклої лінійної комбінації матриць перестановки. Матриці Адамара, означення, ортогональність рядків (стовпців), операції, інші властивості. Перетворення і еквівалентність матриць Адамара. Твердження про порядок матриць Адамара
Розділ 6. Елементи класичної теорії ймовірностей	
17	Підстановки степеня n . Операції на підстановках. Симетрична група підстановок. Степені підстановки. Рівняння з підстановками. Орбіта елемента підстановки. Граф підстановки. Циклова структура. Порядок підстановки. Підгрупи симетричної групи.
18	Комбінаторні схеми. Підгрупи симетричної групи і еквівалентність відображень та комбінаторних перетворень. Загальна комбінаторна схема. Несиметричні комутативні і некомутовативні n -базиси. Симетричні комутативні і некомутовативні n -базиси

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Задачі на класичні імовірності
2	Задачі на класичні імовірності. Дерева рішень, імовірнісні схеми
3	Умовна імовірність, формула повної імовірності
4	Формула Баєса та її застосування
5	Випадкові величини та їх розподіли. Класичні розподіли: розподіл Бернуллі, біноміальний розподіл, геометричний розподіл
6	МКР, частина 1
7	Класичні розподіли: розподіл Пуассона, обернений біноміальний розподіл, гіпергеометричний розподіл.
8	Математичне сподівання та дисперсія випадкових величин. Доведення нерівностей, які оцінюють поведінку випадкових величин (нерівність Маркова, нерівність Чебишова)
9	Генератриси випадкових величин та їх застосування. Моменти та кумулянти випадкових

	величин
10	Символи Ландау та їх властивості. Нотація Кнута
11	МКР, частина 2
12	Гармонічні числа та їх властивості
13	Числа Бернуллі, поліноми Бернуллі та їх властивості
14	Застосування формули Ойлера-Маклорена
15	Спеціальні матриці: пряма сума, прямий добуток матриць; перестановочні матриці, стохастичні та двічі стохастичні матриці
16	Матриці Адамара та їх властивості
17	МКР, частина 3
18	Підсумкове консультативне заняття

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до самостійних та модульних контрольних робіт.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу за темою «Комбінаторні алгоритми». Для підготовки до виконання розрахункової роботи слід скористатися рекомендованою літературою та конспектом лекцій. Студенту надається не менше двох тижнів на виконання розрахункової роботи, після чого в узгоджений із викладачем час студент повинен захистити виконану роботу.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опанувати самостійно.

Календарний рубіжний контроль

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Календарний контроль базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Оголошення результатів контрольних заходів

Результати виконання домашніх завдань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження.

Результати модульної контрольної роботи вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Захист виконаної та оформленої розрахункової роботи проводиться у формі співбесіди з викладачем. Під час захисту студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами задач. Результати виконаної та повністю оформленої роботи у встановлений викладачем термін кожен студент захищає індивідуально. Результати захисту оголошуються кожному студенту окремо у присутності або в дистанційній формі та супроводжуються позитивними коментарями та зауваженнями стосовно помилок.

Результати письмової частини іспиту вказуються на бланках для письмової екзаменаційної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини іспиту оголошуються наприкінці її проходження.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа, рейтингової системи оцінювання та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Виконання домашніх завдань	2	1	≥ 4	8
2.	Модульна контрольна робота	52	1	1	42
3.	Розрахункова робота	10	1	1	10
4.	Іспит	40	1	1	40
Усього					100

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестру. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Семестрова атестація (іспит) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Необхідними умовами допуску є семестровий рейтинг не менше 25 балів та успішний захист розрахункової роботи.

Рейтингова оцінка складається з результатів роботи в семестрі та результатів усного іспиту. Іспит включає в себе практичну частину (3 задачі, 20 балів) та теоретичну частину (2 питання з різних змістовних частин курсу, 20 балів). Під час іспиту забороняється використання будь-яких додаткових довідкових матеріалів.

Студенти, які протягом семестру отримали від 10 до 25 балів, не допускаються до складання іспиту. Замість іспиту такі студенти виконують письмову допускну роботу (10 задач, 20 балів), результати якої додають до семестрового рейтингу; якщо після виконання допускної роботи семестровий рейтинг стає більшим 25 балів, студент допускається до семестрової атестації на перескладанні, а його семестровий рейтинг вважається таким, що дорівнює 25 балів; в іншому випадку результати допускної роботи анулюються, а на перескладанні студент повторно виконує допускну роботу.

Перескладання дисципліни проходить у такій само формі, як і іспит. На перескладанні результати основного іспиту анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів перескладання.

Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізованої атестаційної комісії. Формат повторного перескладання визначається комісією.

Студенти, які протягом семестру одержали менше 10 балів, не здали без поважних причин колоквіум та/або не захистили без поважних причин домашню контрольну роботу, не допускаються до складання семестрової атестації та рекомендуються кафедрі на відрахування.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Склали: професор кафедри ММЗІ, д.ф.-м.н., доц., чл.-кор. НАНУ Савчук Михайло Миколайович, доцент кафедри ММЗІ, к.т.н. Яковлев Сергій Володимирович.

Ухвалено кафедрою математичних методів захисту інформації (протокол №6 від 22.06.2022 р.).

Затверджено Методичною комісією НН ФТІ (протокол № 6 від 30.06.2022 року)