МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря СІКОРСЬКОГО»

ЗАТВЕРДЖУЮ
Голова Вченої ради
Фізико-технічного інституту

О.М.Новіков
«_____»_____2017 р.

ПРОГРАМА ВСТУПНОГО ІСПИТУ

третього (освітньо-наукового) рівня вищої освіти для здобуття наукового ступеня доктор філософії

ГАЛУЗЬ ЗНАНЬ **11 Математика і статистика**
СПЕЦІАЛЬНІСТЬ **113 Прикладна математика**

Ухвалено Вченою радою Фізико-технічного інституту
(протокол від «22» березня 2017 р. № 3 /2017)

Київ
НТУУ «КПІ
2017

Розробники програми:

Савчук Михайло Миколайович	доктор фізико-математичних наук, доцент, в.о. завідувача кафедри математичних методів захисту інформації	_____
Грайворонський Микола Владленович	кандидат фізико-математичних наук, доцент, в.о. завідувача кафедри інформаційної безпеки	_____
Смирнов Сергій Анатолійович	кандидат фізико-математичних наук, с.н.с., доцент кафедри інформаційної безпеки	_____
Яковлєв Сергій Володимирович	кандидат технічних наук, старший викладач кафедри математичних методів захисту інформації	_____

ЧАСТИНА 1

РОЗДІЛ 1 ТЕОРІЯ ЙМОВІРНОСТЕЙ, МАТЕМАТИЧНА СТАТИСТИКА ТА ВИПАДКОВІ ПРОЦЕСИ

1. Загальне поняття випадкової події та стохастичного експерименту, випадкової величини та вектора; функції розподілу; незалежні випадкові величини. Послідовності випадкових величин: поняття збіжності послідовності випадкових величин; нерівність Чебишева; закон великих чисел.
2. Слабка збіжність випадкових величин; генератриси та характеристичні функції випадкових величин; схема незалежних випробувань Бернуллі, граничні теореми Пуассона та Муавра-Лапласа; центральна гранична теорема.
3. Основні поняття математичної статистики: вибірка, варіаційний ряд та емпірична функція розподілу; вибіркові характеристики; асимптотичний розподіл вибіркових моментів; порядкові статистики.
4. Оцінки невідомих параметрів розподілу: класифікація оцінок; незміщені оцінки з мінімальною дисперсією; принцип достатності та оптимальні оцінки; оцінки найбільшої правдоподібності; метод моментів; довірчі інтервали та інтервальне оцінювання.
5. Статистичні гіпотези та статистичні критерії. Критерії згоди; перевірка гіпотези про вигляд розподілу, критерій χ^2; параметричні гіпотези; вибір з двох простих гіпотез; критерій Неймана-Пірсона; критерій відношення правдоподібності.
6. Математичні моделі теорії випадкових процесів: означення випадкових процесів; скінченновимірна функція розподілу випадкового процесу; математичне сподівання, дисперсія, кореляційні функції.
7. Неперервність, похідна та інтеграл випадкового процессу. Види збіжності та неперервності випадкових процесів; математичне сподівання та кореляційна функція похідної та інтегралу.
8. Випадкові процеси Маркова, ланцюги Маркова, рівняння Чепмена-Колмогорова; однорідний випадковий процес Пуассона; вінерівський випадковий процес; гауссівські процеси; стаціонарні випадкові процеси, спектральна теорія; ергодичні теореми випадкових процесів.

РОЗДІЛ 2 МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

1. Універсальна схема моделювання нелінійних динамічних систем.
2. Неперервні системи керування. Принцип суперпозиції, лінійна ланка. Імпульсні перехідні та передаточні функції, частотні характеристики.
3. Алгебра передаточних функцій: правила з'єднання та перетворення. Принцип однонаправленості.
4. BIBO-стійкість. Критерій Михайлова. Ознака чергування коренів.
5. Структурні схеми, сигнальні графи. Визначник графу, формула Мейсона.
6. Фізична реалізовність передаточних функцій. Схеми з підсилювачами та інтеграторами. Канонічна форма спостережуваності.
7. Задача реалізації для передаточних функцій. Канонічні форми.
8. Генерація випадкових чисел з визначеним розподілом, моделювання випадкових подій.
9. Мережі Петрі, графічне та аналітичне зображення, основні задачі та характеристики.
10. Стратегічне і тактичне планування експериментів. Факторні експерименти.

ЧАСТИНА 2

РОЗДІЛ 3 МОДЕЛІ ТА МЕТОДИ ПРИЙНЯТТЯ РІШЕНЬ

1. Багатокритеріальні рішення. Метод лінійної згортки. Домінування за Парето, множина Парето її властивості та побудова.
2. Функції вибору (ФВ) та БВ. Механізми вибору за блокуванням та домінуванням, скалярний та сукупно-екстремальний, мажорітарний та лексікографічний, відповідні функції вибору.
3. Нормальні ФВ. Теорема о непорожності нормального вибору. Структура нормального вибору, число НФВ.
4. Колективні рішення, вибір за більшістю. Парадокс Кондорсе і метод Борда. Аксіоми Ерроу, теорема неможливості і правило диктатора.
5. Правила вибору, змістовні за Кондорсе: Копленда, Сімпсона, Шульце. Утилітаризм та егалітаризм, колективні функції корисності.
6. Функції корисності (ФК) в задачах вибору. Задачі з урнами. Згортання дерева рішень.
7. Криві та мапи байдужості, локальні коефіцієнти заміщення (ЛКЗ). Побудова ФК та прийняття рішення за ЛКЗ.

РОЗДІЛ 4 РІШЕННЯ В УМОВАХ НЕВИЗНАЧЕНОСТІ

1. Системна постановка задачи прийняття рішення (ЗПР). Види невизначеності. Класифікація ЗПР.
2. Формальна структура прийняття рішень в умовах невизначеності. Матриця рішень. Корисність рішення, оцінювальна функція. Оптимістична, нейтральна, песимістична позиція. Відносний песимізм.
3. Геометрична інтерпретація ПР. УТ і АУТ., Поле корисності рішення. Конус переваги і антіконус, області невизначеності. Лінія рівня і функції переваги.
4. Класичні критерії ПР: мінімаксний (MM), Баєса-Лапласа (BL), Севіджа (S), узагальнений мінімаксний (GMM), умови їх застосовності.
5. Похідні критерії ПР: Гурвіца (HW), Ходжа-Лемана (HL), Гермєйєра (G), умови застосовності.
6. Міра ризику та складові критерії Мушика: BL(MM), BL(S), умови застосовності.
7. Графічне дослідження критеріїв ПР. Зв'язок між критеріями ПР. Геометрична оптимізація для MM, G, BL, S. Напрямні та лінії рівня, конуси.
8. Геометрична оптимізація для G, BL, HL, HW, BL (MM).
9. Кількісні характеристики ситуації ПР. Незалежні і контрольовані змінні. Класифікація видів завдання параметрів. Детерміноване і стохастичне поведінку оточення. Інформованість. Витрати на інформацію. Спостереження до моменту ПР і повторні реалізації рішення.
10. Оцінка значущості незалежного параметра. Абсолютна і відносна релевантність незалежного параметра. Ентропія параметра, як характеристика його інформативності, формула Шеннона. Перенесення формули ентропії на безперервні випадкові величини.
11. Ранжування незалежних параметрів за значимістю, вибір інтервалів дискретизації.
12. Метод Ханселя. Зворотній зв'язок ентропії з числом групи. Методи розрахунку: ітераційний та від мінімальної релевантності.
13. Модифікований метод Ханселя. Процедура та її збіжність.
14. Дискретизація за функцією розподілу.
15. Три ситуації ПР, постановка завдання ПР: помилка вибору, розмір емпіричної і апостеріорної вибірок, критерії.
16. Квантилі, інтервальні оцінки. Схема Бернуллі і розподіл Бернуллі.
17. Емпірична ситуація ПР. Редукція до задачі ЛП.
18. Прогностична ситуація ПР. Редукція до задачі ЛП.
19. Емпірико-прогностична ситуація ПР. Редукція до задачі ЛП.

20. Рішення допоміжної задачі лінійного програмування (ЛП).
21. Багатокритеріальне ПР з інтервальними оцінками ваг критеріїв.

РОЗДІЛ 5 ВСТУП ДО НЕЛІНІЙНОГО АНАЛІЗУ

1. Фазовий простір. Динамічні системи (ДС). Фазові траєкторії. Класифікація моделей ДС: модель-потік, модель-відображення. Дисипативні та консервативні системи (умови дисипативності).
2. Стійкість ДС: типи стійкості, показники Ляпунова, умови стійкості для системи-потоку та системи-відображення.
3. Біфуркація. Точки біфуркації. Простір параметрів. Елементарні катастрофи як біфуркації кількості особливих точок. Структурна стійкість і теорія катастроф Рене Тома.
4. Відображення. Перехід від моделі-потоку до моделі-відображення. Переріз Пуанкаре. Загальні властивості унімодального відображення $x_{n+1} = f(x_n)$.
5. Логістичне відображення (відображення Фейгенбаума) та його властивості при різних значеннях параметра. Біфуркації народження циклів (подвоєння періоду).
6. Хаотичний рух в динамічних системах (ДС-потік, ДС-відображення). Моделювання випадковими процесами. Сценарії виникнення хаосу (сценарій Фейгенбаума, перехід до хаосу через переміжуваність (рос. «перемежаемость»)).
7. Самоподібність і фрактальна структура як ознака детермінованого хаосу динамічних систем. Приклади фрактальних множин. Фрактальні розмірності. Дивний аттрактор (аттрактор Лоренца, його фрактальна структура).

ЧАСТИНА 3

РОЗДІЛ 6 КОМБІНАТОРНИЙ АНАЛІЗ

1. Комбінаторні операції та схеми. Алгебраїчні та кардинальні операції над множинами та мультимножинами. Потужність множин та мультимножин. Розміщення з повторенням/без повторення, вибірки без повернення та з поверненням, перестановки без повторень та з повтореннями, розбиття множин.

2. **Генератриси (твірні функції) послідовностей.** Звичайні та експоненційні генератриси. Операції над генератрисами (сума, згортка, похідна, інтеграл). Визначення елементів послідовностей за їх генератрисами. Побудова генератриси лінійної рекурентної послідовності. Пошук розв'язків лінійних рекурент через корені характеристичного поліному.
3. **Асимптотична поведінка функцій.** Символи Ландау, еквівалентність функцій, ієрархія за швидкістю зростання. Формула Ойлера-Маклорена та її застосування: асимптотичні еквіваленти для гармонійних чисел та для факторіалів (формула Стірлінга).
4. **Комбінаторні алгоритми.** Генерація перестановки за індексом, із мінімальними змінами, у лексикографічному порядку. Генерація підмножин за індексом, у лексикографічному порядку; коди Грея, генерація підмножин із мінімальними змінами. Вибір випадкової перестановки та випадкової підмножини.

РОЗДІЛ 7 ПРИКЛАДНА АЛГЕБРА

1. **Основні поняття прикладної алгебри.** Визначення півгрупи, моноїда, групи, абелевої групи. Порядок групи, порядок елементу групи, циклічні підгрупи. Теорема Лагранжа. Визначення кільця, ідеалу кільця, поля.
2. **Кільце лишків за модулем *n*.** Визначення, операції над лишками. Алгоритм Евкліда та розширений алгоритм Евкліда. Мультиплікативна група кільця лишків, функція Ойлера та її обчислення. Теорема Ойлера, мала теорема Ферма. Розв'язування лінійних порівнянь.
3. **Квадратичні лишки.** Символи Лежандра та Якобі, правила обчислення, критерій Ойлера. Пошук квадратних коренів за простим модулем та за модулем виду $p \cdot q$.
4. **Перевірка натуральних чисел на простоту.** Тест Ферма, числа Кармайкла. Тест Соловея-Штрассена. Тест Міллера-Рабіна.
5. **Скінченні поля характеристики 2.** Способи побудови поля та представлення елементів поля (вектори, поліноми), подання операцій над елементами. Операції у поліноміальному та нормальному базисах (додавання, множення, піднесення до степеня, пошук оберненого елементу, обчислення сліду).

РОЗДІЛ 8 КРИПТОГРАФІЯ ТА КРИПТОАНАЛІЗ

1. **Основні поняття криптології.** Задачі, напрямки та методи захисту інформації. Криптографічний захист інформації. Основні поняття криптології. Моделі джерел відкритого тексту, ентропія на символ джерела. Загальна класифікація класичних і сучасних шифрів. Класичні схеми шифрування.
2. **Теория секретних систем Шеннона.** Иерархия типов атак на криптосистему. Теоретична та практична стійкість. Ентропія. Цілком таємні криптосистеми. Границя Шеннона. Ненадійність ключа і відкритого тексту Відстань однозначності. Принципи Шеннона побудови стійких шифрів.
3. **Булеві функції та випадкові послідовності.** Булеві функції та способи їх зображення. Криптографічні властивості булевих функцій. Методи генерації випадкових та псевдовипадкових послідовностей. Статистичні методи оцінки якості булевих функцій, випадкових та псевдовипадкових послідовностей.
4. **Системи блокового та потокового шифрування.** Схема Фейстела. Стандарти блокового шифрування DES. ГОСТ 28147-89, Rijndael. Регістри зсуву з лінійним зворотним зв'язком. Способи введення нелінійності у схеми потокового шифрування на регістрах зсуву з лінійним зворотним зв'язком.
5. **Теоретичні основи асиметричної криптографії.** Математичні моделі алгоритмів. Визначення часової та ємкісної складності алгоритмів, поліноміальної і експоненціальної складності. Розв'язувальні і важкорозв'язувальні задачі, класи P і NP. Поліноміальна звідність. NP-повні задачі. Проблема існування односторонніх функцій в класичній та постквантовій моделях обчислень.
6. **Складність алгоритмів та односторонні функції.** Односторонні функції, односторонні функції з секретом. Схема відкритого розподілу ключів Діффі і Хеллмана. Односторонні функції RSA, Рабіна. Оцінки складності обчислення та обернення функцій.
7. **Системи шифрування асиметричної криптографії.** Загальна концепція асиметричних систем шифрування з відкритими ключами. Системи шифрування Мессі-Омури та Эль-Гамаля. Криптосистеми RSA та Рабіна.
8. **Хеш-функції.** Криптографічні властивості. Загальні схеми побудови. Колізії хеш-функцій. Оцінки ймовірностей колізій та трудомісткості їх побудови. Застосування хеш-функцій.
9. **Цифровий підпис.** Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з хеш-функцією в асиметричної криптографії.

Цифровий підпис у схемі RSA з використанням хеш-функцій, цифрові підписи Эль-Гамаля, Рабіна. Сліпий підпис. Атаки на цифровий підпис.

10. **Криптографічні протоколи.** Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Криптографічні алгоритми автентифікації: парольна автентифікація, автентифікація з використанням симетричних и асиметричних криптосистем.
11. **Цілі та підходи** в **криптоаналізу**. Теоретико-інформаційний, байєсівський підхід, системний, семантичний підхід, доказова стійкість та інші. Класифікація атак на криптографічні системи і протоколи захисту інформації.

Критерії оцінювання фахового випробування для вступу на третій рівень вищої освіти для здобуття наукового ступеня доктор філософії за спеціальністю 113 "Прикладна математика"

Відповідь на кожне теоретичне питання комплексного фахового випробування оцінюється за бальною шкалою за таким порядком визначення:

- 24…25 – правильна, вичерпна відповідь, обсяг виконання 95-100%;
- 21…23 – повна відповідь (містить не менше 85% потрібної інформації);
- 19…20 – достатньо повна відповідь (містить не менше 75% потрібної інформації, або незначні неточності);
- 17…18 – достатня відповідь (містить не менше 65% потрібної інформації або значні неточності);
- 15…16 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації або окремі помилки);
- менше 15 – незадовільна відповідь.

Система оцінювання практичного запитання (задачі):

- 24…25 – повне (обсяг виконання 95-100%), безпомилкове, відмінне розв'язання завдання;
- 21…23 – повне розв'язання завдання з несуттєвими похибками, містить не менше 85% потрібної інформації;
- 19…20 – розв'язання завдання з похибками, містить не менше 75% потрібної інформації;

- 17…18 – завдання виконане задовільно, з невеликими помилками, містить не менше 65% потрібної інформації;
- 15…16 – завдання виконане задовільно, з помилками, містить не менше 60% потрібної інформації;
- менше 15 – завдання не виконано.

Кінцева кількість балів – сума балів, отриманих за відповіді на кожне з трьох вищезазначених питань та практичне завдання. Максимальна кількість балів – 100.

Переведення значення бальної шкали в екзаменаційну оцінку здійснюється за такою системою співвідношення (згідно з Положенням НТУУ «КПІ» про прийом на навчання за освітньо-професійними програмами):

Сумарна кількість балів	Оцінка ECTS	Чисельний еквівалент оцінки з фахового випробування
95…100	**A**	5,0
85…94	**B**	4,5
75…84	**C**	4,0
65…74	**D**	3,5
60…64	**E**	3,0
Менше 60	**F**	0