НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Затверджено Вченою Радою
Фізико-технічного інституту
Протокол № _____ від _____ 20__ р.
Голова Ради ФТІ_____О.М. Новіков
М.П.

.

ПРОГРАМА

комплексного фахового випробування для вступу на навчання за освітньо-професійними програмами підготовки магістра
за спеціальністю 113 «Прикладна математика»

Програму рекомендовано кафедрою
математичних методів захисту інформації
Протокол № ___ від _____ 20__ р.
В.о. зав. кафедри _____ М. М. Савчук

Київ – 2017 р.

ВСТУП

Програма комплексного фахового випробування для вступу на освітньо-професійну програму підготовки магістра/спеціаліста за спеціальністю 113 «Прикладна математика» складена на основі освітньо-професійної програми напряму підготовки 113 «Прикладна математика».

Програма побудована з наступних розділів: загальна (спільна) частина, та варіативні частини, відповідно до спеціалізацій.

Програма розроблена згідно з навчальними програмами нормативних навчальних дисциплін:

- «Теорія ймовірностей»,
- «Математична статистика»,
- «Випадкові процеси»,
- «Числові методи»,
- «Математичне моделювання»,
- «Теорія керування»,
- «Онови нелінійного аналізу»,
- «Моделі та методи прийняття рішень»,
- «Загальна теорія безпеки»,
- «Конкурентна розвідка»,
- «Комбінаторний аналіз»,
- «Прикладна алгебра»,
- «Спеціальні розділи обчислювальної математики»,
- «Симетрична криптографія»,
- «Асиметричні криптосистеми та протоколи».

Комплексне фахове випробування здійснюється в письмовій формі. Білет містить чотири питання (два теоретичні та два практичні з різних розділів програми).

Тривалість комплексного фахового випробування – 2 астрономічні години, перерви немає. Екзаменований вільно розподіляє свій час між всіма завданнями.

РОЗДІЛ «ТЕОРІЯ ЙМОВІРНОСТЕЙ, МАТЕМАТИЧНА СТАТИСТИКА ТА ВИПАДКОВІ ПРОЦЕСИ»

Теоретична частина

1. **Загальне поняття** випадкової події та стохастичного експерименту, випадкової величини та випадкового вектора; функції розподілу; незалежні випадкові величини; дискретні та неперервні випадкові величини та їх характеристики.

2. **Послідовності випадкових величин:** поняття збіжності послідовності випадкових величин; нерівність Чебишева; закон великих чисел.

3. **Граничні теореми теорії ймовірностей:** слабка збіжність випадкових величин; генератриси та характеристичні функції випадкових величин; схема незалежних випробувань Бернуллі, граничні теореми Пуассона та Муавра-Лапласа; центральна гранична теорема.

4. **Основні поняття математичної статистики:** вибірка, варіаційний ряд та емпірична функція розподілу; вибіркові характеристики; асимптотичний розподіл вибіркових моментів; порядкові статистики; розподіли деяких функцій від нормальних випадкових величин.

5. **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.

6. **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; складні гіпотези; критерій відношення правдоподібності.

7. **Математичні моделі теорії випадкових процесів:** означення випадкових процесів; скінченновимірна функція розподілу випадкового процесу; математичне сподівання, дисперсія, кореляційна функція, нормована кореляційна функція, взаємна кореляційна функція випадкового процесу та їх властивості.

8. **Неперервність, похідна та інт**еграл випадкового процесу: види збіжності та неперервності випадкових процесів; математичне сподівання та кореляційна функція похідної та інтегралу.

9. **Випадкові процеси**: Маркова, ланцюги Маркова, рівняння Маркова; марковські дискретні процеси з неперервним часом, рівняння Чепмена-Колмогорова; однорідний випадковий процес Пуассона; вінерівський випадковий процес; гауссівські процеси; стаціонарні випадкові процеси, спектральна теорія; ергодичні теореми випадкових процесів.

Практична частина

1. Кількісні характеристики дискретних випадкових величин. Задачі на біноміальний розподіл, геометричний, гіпергеометричний розподіл, розподіл Пуассона.

2. Неперервні випадкові величини та вектори, їх властивості та характеристики.

3. Критерії перевірки гіпотези про вигляд розподілу, про однорідність вибірки та гіпотези про незалежність. Вибір з двох простих гіпотез.

4. Властивості та характеристики ланцюгів Маркова, випадкового процесу Пуассона, вінерівского, гауссівських випадкових процесів.

РОЗДІЛ «ЧИСЛОВІ МЕТОДИ»

Теоретична частина

1. Розв’язання нелінійних рівнянь: теорема про кільце, про верхню межу, теорема Штурма, методи бісекції, хорд, Ньютона.

2. Розв’язання СЛАР: метод вибору головного елемента, єдиного ділення, квадратного кореня, простої ітерації та Зейделя.

3. Розв’язання систем нелінійних алгебраїчних рівнянь: метод простої ітерації, Ньютона для систем двох та n рівнянь. Поняття принципу стиснених відображень.

4. Обчислення власних чисел та векторів матриць: методи Данілевського, Якобі, Крилова, степеневий метод.

5. Інтерполяційний поліном Лагранжа, перша та друга інтерполяційні формули Ньютона.

6. Числові методи розв'язання задачі Коші та крайових задач для системи звичайних диференційних рівнянь: методи Ейлера, Рунге-Кутта та Адамса, метод скінчених різниць.

7. Числові методи розв'язання крайових задач для систем диференційних рівнянь у часткових похідних: метод побудови явних та неявних різницевих схем для рівнянь теплопровідності, методи побудови скінчено-різницевих схем для рівнянь гіперболічного, еліптичного типу, поняття про метод скінчених елементів.

Практична частина

1. Розв'язання систем рівнянь методом простої ітерації.
2. Метод скалярних добутків знаходження власних значень матриць.
3. Інтерполяційна формула Лагранжа.
4. Метод Ейлера розв'язання задачі Коші.

РОЗДІЛ «МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ»

Теоретична частина

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. Методи генерації випадкових чисел: монетарний, мультипликативний та квадратичний.

9. Генерація випадкових чисел з визначеним розподілом.

10. Моделювання випадкових подій.

11. Мережі Петрі, графічне та аналітичне зображення, основні задачі та характеристики.

12. Стратегічне і тактичне планування експериментів. Факторні експерименти. Латинський план.

Практична частина

1. Розрахунок ПФ за сигнальним графом. Реалізація ПФ сигнальним графом.
2. Аналіз стійкості поліномів.
3. Побудова генераторів випадкових чисел з визначеним розподілом.
4. Знаходження сумісно можливих подій та мови подій за мережею Петрі.
5. Побудова факторних планів експериментів.

РОЗДІЛ «ТЕОРІЯ КЕРУВАННЯ»

Теоретична частина

1. Поняття систем керування: основні визначення та класифікація систем керування. Поняття математичної моделі керованих процесів.
2. Метод простору станів. Приклади представлення математичних моделей у формі простору станів.
3. Стійкость систем автоматичного керування. Аналіз стійкості лінійних систем на основі функцій Ляпунова.
4. Аналіз стійкості лінійних систем за коренями характеристичного рівняння.
5. Керованість та спостережуваність систем автоматичного керування.
6. Оптимальне керування лінійним об`єктом з квадратичним критерієм. Рівняння Рікаті та його інтегрування.
7. Принцип максимуму Л.С. Понтрягіна. Синтез системи оптимального керування з обмеженнями на керуючі впливи.

Практична частина

1. Аналіз стійкості ЛС за коренями характеристичного рівняння та по функції Ляпунова.
2. Визначення керованості та спостережуваності ЛС.
3. Задачі оптимального керування на принцип максимуму.

ВАРІАТИВНИЙ РОЗДІЛ ДЛЯ СПЕЦІАЛІЗАЦІЇ «МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ»

ОСНОВИ НЕЛІНІЙНОГО АНАЛІЗУ

Теоретична частина

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).

Практична частина

1. Вправи на знаходження та дослідження фазових траєкторій ДС на площині.
2. Вправи на лінеаризацію ДС та їх дослідження за допомогою характеристичних показників.
3. Знаходження операторів еволюції простих ДС.
4. Вправи на побудову відображення послідовності ДС.
5. Вправи на визначення показників Ляпунова та інших характеристик випадкових процесів для простих відображень (типу Бернуллі).
6. Вправи на визначення фрактальних (дробових) розмірностей простих фракталів (множина Кантора, килим Серпінського та ін.).

МОДЕЛІ ТА МЕТОДИ ПРИЙНЯТТЯ РІШЕНЬ

Теоретична частина

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.

Практична частина

1. Багатокритеріальна оптимізація (Парето, лінійна згортка, лексикографічна).
2. Обчислення значень нормальних функцій вибору.
3. Визначення переможця за профілем переваг.
4. Оптимізація функції корисності за відомим ЛКЗ.

ВАРІАТИВНИЙ РОЗДІЛ ДЛЯ СПЕЦІАЛІЗАЦІЇ «АНАЛІТИЧНІ МЕТОДИ БЕЗПЕКИ ІНФОРМАЦІЇ»

ТЕОРІЯ БЕЗПЕКИ ТА КОНКУРЕНТНА РОЗВІДКА

Теоретична частина

1. Поняття «безпека», «загроза» та «ризик» як системоутворюючі категорії загальної теорії безпеки
2. Безпека як властивість складних систем
3. Методи побудови F/N-діаграм
4. Загальносистемні закони безпеки складних систем
5. Гомеостазис як модель оцінки стану захищеності складних систем
6. Аналітична процедура моніторингу конкурентної розвідки: аналіз *Z*-діаграм
1. Кількісна оцінка конкурентного середовища за допомогою *M*-діаграм («павук»-діаграми)
7. Google-аналітика як засадничий метод дослідження конкурентної розвідки
8. Невизначість та ризик
9. Оцінка індивідуальних ризиків
10. Оцінка колективних ризиків
11. Матриця прогнозованого ризику: застосування та методи побудови
12. Управління ризиком: концепція «прийнятного ризику»
13. Стратегія оцінки ризикованих альтернатив

Практична частина

1. Здійснити ієрархічну декомпозицію системи забезпечення кібернетичної безпеки на прикладі.
2. Побудувати матрицю інцидентності в системі «загрози – механізми відвертання» на прикладі.
3. Розглядаються два варіанти системи енергозбереження об’єкту. Відомі ймовірності аварії та можливий збиток у обох варіантів. Який проект є переважним з погляду безпеки?
4. Знайти коефіцієнт варіації виплат згідно договору страхування життя впродовж року. Страхова сума та ймовірність страхового випадку року відомі.
5. У деякому місті річні втрати від негараздів є незалежними випадковими величинами з відомим розподілом. Знайти ймовірність того, що максимальний із збитків буде більшим деякої величини.
6. Фірмі запропоновано два альтернативні проекти (А і В), аналіз яких показав, що рівень їх доходності може бути наступним:

для першого проекту

Дохід (тис грн.)	Ймовірність одержання
250	*a*
350	*b*
450	*c*

для другого проекту

Доход (тис грн.)	**Ймовірність одержання**
200	*d*
350	*e*
500	*f*

Визначити найменш ризикований з двох проектів.

7. Фірмі запропоновано два альтернативні проекти (A і B), середні сподівані доходи яких відомі. Крім того відомі стандартні відхилення для обох проектів. Необхідно визначити найменш ризикований з даних проектів.

8. Для лотереї $L(0, p, 10)$ та функції корисності $u(x)$ знайти детермінований еквівалент лотереї та перевірити особу, що ухвалює рішення на схильність до ризику.

МОДЕЛІ ТА МЕТОДИ ПРИЙНЯТТЯ РІШЕНЬ

Теоретична частина

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.

Практична частина

1. Багатокритеріальна оптимізація (Парето, лінійна згортка, лексикографічна).
2. Обчислення значень нормальних функцій вибору.
3. Визначення переможця за профілем переваг.
4. Оптимізація функції корисності за відомим ЛКЗ.

ВАРІАТИВНИЙ РОЗДІЛ ДЛЯ СПЕЦІАЛІЗАЦІЇ «МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

КОМБІНАТОРНИЙ АНАЛІЗ

Теоретична частина

1. **Комбінаторні операції.** Алгебраїчні та кардинальні операції над множинами та мультимножинами. Потужність множин та мультимножин, теореми про потужність булеану. Принцип включення-виключення, його застосування.
2. **Основні комбінаторні конфігурації.** Розміщення з повторенням/без повторення, вибірки без повернення/з поверненням, перестановки без повторень/з повторенням, розбиття множин. Перелічування основних комбінаторних конфігурацій. Біном Ньютона.
3. **Генератриси (твірні функції) послідовностей.** Звичайні та експоненційні генератриси. Операції над генератрисами (сума, згортка, похідна, інтеграл). Визначення елементів послідовностей за їх генератрисами.
4. **Лінійні рекурентні послідовності.** Побудова генератриси лінійної рекурентної послідовності. Формула Біне загального елементу послідовності Фібоначчі. Пошук розв’язків лінійних рекурент через корені характеристичного поліному.
5. **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).
6. **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.

Практична частина

1. Задачі на підрахунок числа комбінаторних конфігурацій, потужності множин.
2. Комбінаторні задачі, пов’язані з застосуванням поліномів і генератрис, доведення комбінаторних тотожностей.
3. Задачі на застосування асимптотичних співвідношень, формули Стірлінга, гармонічних чисел в комбінаторному аналізі.
4. Задачі на комбінаторні алгоритми породження перестановок та підмножин в лексикографічному порядку, випадкових перестановок та підмножин.

ПРИКЛАДНА АЛГЕБРА, СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

Теоретична частина

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).

6. **Регістри зсуву із лінійним зворотним зв'язком.** Подання лінійних регістрів зсуву діаграмою, рекурентою, супроводжуючою матрицею та характеристичним поліномом. Визначення періоду послідовності, яку генерує лінійний регістр зсуву. Циклова структура рекурентної послідовності.

Практична частина

1. Задачі на пошук обернених елементів за модулем, розв'язування лінійних порівнянь.
2. Знаходження квадратних коренів за простим модулем та за модулем виду $p \cdot q$.
3. Задачі на виконання операцій у скінченному полі характеристики 2.

СИМЕТРИЧНА КРИПТОГРАФІЯ

Теоретична частина

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.

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. Класичні схеми шифрування. Моноалфавітні підстановки. Методи криптоаналізу. Поліалфавітні підстановки. Шифр Віженера та його криптоаналіз. Інші шифри підстановки. Шифри перестановки: загальне визначення, табличні

перестановки, маршрути Гамільтона, грати Кардано інші шифри перестановки. Комбіновані шифри.

4. 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.

5. Системи блокового шифрування. Схема Фейстела. Стандарт блокового шифрування DES. ГОСТ 28147-89 та інші шифри фейстелівської та модифікованої фейстелівської схеми. Алгоритм блокового шифрування Rijndael. Режими використання блокових шифрів.

6. Потокові системи шифрування. Регістри зсуву з лінійним зворотним зв'язком. Способи введення нелінійності у схеми потокового шифрування на регістрах зсуву з лінійним зворотним зв'язком. Схеми з нерівномірним рухом регістрів зсуву. Приклади сучасних потокових шифрів: A5/1, LILI 128, RC4. Новітні тенденції у синтезі потокових систем шифрування.

Практична частина

1. Задачі математичної теорії інформації та теорії секретних систем Шеннона.
2. Вправи на класичні шифри підстановки та перестановки.
3. Криптографічні властивості булевих функцій.
4. Визначення властивостей потокових симетричних шифрів.

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ

Теоретична частина

1. 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.

2. Складність алгоритмів та односторонні функції. Односторонні функції, односторонні функції з секретом. Одностороння функція дискретного піднесення до степеня. Схема відкритого розподілу ключів Діффі і Хеллмана. Односторонні функції RSA, Рабіна. Оцінки складності обчислення та обернення функцій.

3. Системи шифрування асиметричної криптографії. Загальна концепція асиметричних систем шифрування з відкритими ключами. Системи шифрування Мессі-Омури та Эль-Гамаля. Криптосистеми RSA та Рабіна. Основа стійкості асиметричних систем шифрування.

4. Хеш-функції. Криптографічні властивості. Загальні схеми побудови. Характеристики хеш-функцій, найбільш уживаних у системах захисту інформації. Колізії хеш-функцій. Математичні моделі оцінки ймовірностей колізій та трудомісткості їх побудови. Застосування хеш-функцій.

5. 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.

6. 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.

7. Криптосистеми на еліптичних кривих. Групи точок еліптичних кривих: основні означення, групова операція. Криптосистеми на еліптичних кривих, основні питання, що виникають при їх реалізації. Стандарт цифрового підпису на еліптичних кривих ДСТУ 4145-2002.

Практична частина

1. Отримання оцінок складності алгоритмів.
2. Задачі на схему Діффі-Хеллмана розповсюдження ключів повідкритим каналам, алгоритми асиметричного шифрування та цифрового підпису.
3. Задачі на побудову колізій хеш-функцій.
4. Задачі на побудову еліптичних кривих.

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Використання допоміжного матеріалу

Під час відповідей на теоретичні питання користуватися додатковою літературою забороняється. Для розв'язання задач дозволяється користуватися калькулятором.

Критерії оцінювання

На комплексному фаховому випробуванні вступник отримує екзаменаційний білет, який включає чотири питання з переліку зазначених вище тем і розділів навчальних дисциплін: два теоретичних та два практичних. Два питання у білеті (одне теоретичне та одне практичне) стосуються загальної (спільної) частини, інші два – варіативної. Відповідь на кожне питання оцінюється у 25 балів.

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

- 24…25 – правильна, вичерпна відповідь, що містить всі визначення, твердження та доведення (обсяг виконання 95-100%);
- 21…23 – повна відповідь із деякими непринциповими неточностями (містить не менше 85% потрібної інформації);
- 19…20 – достатньо повна відповідь із незначними неточностями у визначеннях та/або доведеннях (містить не менше 75% потрібної інформації);
- 17…18 – достатня відповідь, яка однак містить значні неточності у визначеннях та/або доведеннях (містить не менше 65% потрібної інформації);
- 15…16 – неповна, але задовільна відповідь (містить не менше 60% потрібної інформації, окремі суттєві помилки);
- менше 15 – незадовільна відповідь із грубими помилками (містить менше 60% потрібної інформації).

Відповідь на практичне питання (задачу) комплексного фахового випробування оцінюється за бальною шкалою за таким порядком визначення:

- 24…25 – повне, безпомилкове, відмінне розв'язання завдання (обсяг виконання 95-100%);
- 21…23 – повне розв'язання завдання з несуттєвими описками або помилками, які не впливають на основний зміст розв'язку; розв'язання, яке містить не всі необхідні пояснення (містить не менше 85% потрібної інформації);
- 19…20 – розв'язання завдання з невеликими помилками, які несуттєво впливають на основний зміст розв'язку, або без значної частини необхідних пояснень (містить не менше 75% потрібної інформації;
- 17…18 – завдання виконане задовільно, але із помилками, які впливають на зміст розв'язку, або без суттєвої частини необхідних пояснень (містить не менше 65% потрібної інформації);

- 15…16 – завдання виконане задовільно, з помилками або без необхідних теоретичних пояснень (містить не менше 60% потрібної інформації);
- менше 15 – завдання виконано незадовільно, із грубими помилками, без необхідних пояснень, або не виконано взагалі.

Загальна оцінка за комплексний фаховий екзамен обчислюється як сума балів, отриманих за відповіді на кожне з чотирьох питань білету. 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 магістра і спеціаліста):

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

Типові завдання

Білет № 3

1.Граничні теореми теорії ймовірностей: слабка збіжність випадкових величин; генератриси та характеристичні функції випадкових величин; схема незалежних випробувань Бернуллі, граничні теореми Пуассона та Муавра-Лапласа; центральна гранична теорема.
2. Відображення. Перехід від моделі-потоку до моделі-відображення. Переріз Пуанкаре. Загальні властивості унімодального відображення $x_{n+1} = f(x_n)$.
3. Дослідити стійкість поліному: $p^5 + 4p^4 + 5p^3 + 4p^2 + 3p + 1$.
4. Задано ЛКЗ y3/x5 , визначити найкращу з альтернатив A(1,3); B(2,2); C(3,1)

Список літератури

1. В.Феллер. Введение в теорию вероятностей и ее приложения, т. 1,2. - Москва: Мир, 1964
2. А.Н.Ширяев. Вероятность. - Москва: Наука,1980.
3. Ш.Закс. Теория статистических выводов. - Москва: Мир,1975.
4. Д.Кокс, Д.Хинкли. Теоретическая статистика. - Москва: Мир, 1978.
5. А.В.Скороход. Лекції з теорії випадкових процесів: Навч. посібник. - К.: Либідь, 1990. - 168 с.
6. Дж. Ламперти. Случайные процессы. Обзор математической теории. - Киев: Вища школа, 1983.

7. Ю.А.Розанов. Случайные процессы (краткий курс). - Москва: Наука, 1971.
8. Бусленко Н.П. Моделирование сложных систем. - М.: Наука. - 1978. – 400 с.
9. Гультяев А. Визуальное моделирование в среде MATLAB: учебный курс. -СПб: Питер. -2000. -430 с.
10. Филлипс Ч., Харбор Р. Системы управления с обратной связью. –М.: Лаборатория Базовых Знаний. -2001. -616 с.
11. Бенькович Е.С., Колесов Ю.Б., Сениченков Ю.Б. Практическое моделирование динамических систем. –СПБ.: БХВ-Петербург. -2002. -464 с.
12. Ларичев О.И. Теория и методы принятия решений, а также Хроника событий в Волшебных Странах. -М.: Логос. -2000. -296 с.
13. Макаров И.М. и др. Теория выбора и принятия решений. -М.: Наука. -1982. -328 с.
14. Юдин Д.Б. Вычислительные методы теории принятия решений. -М.: Наука. -1989. -320 с.
15. Райзер Г.Дж. Комбінаторная математика. – М.: Мир, 1966. – 154с.
16. Рыбников К.А. Введение в Комбинаторный анализ. – М.: Изд. Моск. ун-та, 1985. – 308с.
17. Грэхем Р., Кнут Д., Паташник О. Конкретная математика. – М.: Мир, 1998. – 703с.
18. Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384с.
19. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы. – М.: Мир, 1980. – 478с.
20. Калужнин Л.А. Введение в общую алгебру. М.:”Наука”, 1973.
21. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: “Мир”, 1976.
22. Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т./ Пер. с англ. – М: Мир, 1988. – Т. 2. – 425с.
23. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.
24. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. - М.: Издательство ТРИУМФ, 2003. - 816 с.
25. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003 – 400с.
26. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
27. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. - М.: Мир, 2006. – 471с.
28. Коблиц Н. Курс теории чисел и криптографии. – М: ТВП,2001 – 254с.
29. Menezes A., P. van Oorschot, S.Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.

Розробники програми

д.ф-м.н. професор Савчук М.М.
д.т.н. професор Качінський А.Б.
к.ф.-м.н. доцент Смирнов С.А.
к.ф-м.н. доцент Кравцов О.В.
к.т.н. ст. викладач Яковлєв С.В.