

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ДНІПРОПЕТРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ОЛЕСЯ ГОНЧАРА  
Факультет прикладної математики  
Кафедра математичного забезпечення ЕОМ

«Затверджую»

Ректор Дніпропетровського  
національного університету  
ім. О. Гончара М.В. Поляков

«14»

2017 р.



«Погоджено»

Проректор  
з науково-педагогічної роботи  
С.О. Чернецький

«13»

13

2017 р.

**ПРОГРАМА**  
**ФАХОВИХ ВСТУПНИХ ВИПРОБУВАНЬ**  
за другим (магістерським) рівнем вищої освіти  
спеціальності 121 – Інженерія програмного забезпечення

Розглянуто на Вченій ради ФПМ  
протокол № 5 від 17.01.2017 р.

Голова Вченої ради ФПМ  
проф. О.М. Кісельова  
«12» 01 2017 р.

Завідувач кафедри  
математичного забезпечення ЕОМ  
О.Г. Байбуз  
"17" січня 2017 р.

Дніпро  
2017 р.

## ПЕРЕЛІК ДИСЦИПЛІН, ЗА ЯКИМИ БУДУТЬ АТЕСТУВАТИСЬ АБІТУРУЄНТИ:

Архітектура комп'ютера, Архітектура та проектування програмного забезпечення, Людино-машинна взаємодія, Моделювання та аналіз програмного забезпечення, Безпека програм та даних, Організація комп'ютерних мереж.

В результаті вивчення дисциплін фахівець повинен знати:

структуру та функції операційних систем, основи побудови людино-машинного інтерфейсу, засоби захисту програм і даних від несанкціонованих дій, структуру та функції комп'ютерних мереж, засоби застосування Інтернет,.

В результаті вивчення дисциплін фахівець повинен вміти:

- володіти методами системного аналізу;
- розробляти специфікації вимог користувачів ;
- здійснювати аналіз вимог, розробляти специфікацію програмних вимог, виконувати їхню верифікацію та атестацію;
- моделювати різні аспекти системи, для якої створюється ПЗ;
- проектувати компоненти архітектурного рішення;
- проектувати людино-машинний інтерфейс;
- володіти основами конструювання ПЗ;
- володіти методами та технологіями організації та застосування даних;
- застосовувати та створювати компоненти багаторазового використання;
- створювати чітку, стислу та точну технічну документацію у відповідності до діючих стандартів;
- використовувати можливості апаратного забезпечення;
- використовувати можливості операційних систем;
- використовувати можливості офісних і мережевих програмних систем;
- забезпечувати захищеність програм і даних від несанкціонованих дій;
- застосовувати математичні знання у процесі розв'язання професійних задач, побудови математичних моделей;
- застосовувати знання в галузі інформатики й сучасних інформаційних технологій та Internet;
- орієнтуватись у схемах алгоритмів, програм, даних і систем;
- використовувати професійно профільовані знання й уміння в галузі практичного використання комп'ютерних технологій;
- використовувати інтернет – ресурси для рішення експериментальних і практичних завдань у галузі професійної діяльності;
- сприймати та розуміти надану інформацію у повному обсягу.

## Структура тестового завдання

Тестове завдання включає тести з вибором однієї правильної відповіді - 4 бали; 0 балів, якщо вказано неправильну відповідь, або вказано більше однієї відповіді, або відповіді не надано.

Завдання складається з 25 тестів:

5 тестів	з дисципліни	Архітектура комп'ютера;
5 тестів	з дисципліни	Архітектура та проектування програмного забезпечення;
5 тестів	з дисципліни	Людино-машинна взаємодія;
4 тести	з дисципліни	Моделювання та аналіз програмного забезпечення;
3 тести	з дисципліни	Безпека програм та даних;
3 тести	з дисципліни	Організація комп'ютерних мереж.

Всього: 25 тестів

**Максимальна можлива загальна сума дорівнює 100 балам та складається  $25 \cdot 4 = 100$ .**

## АРХІТЕКТУРА КОМП'ЮТЕРА

1. Архітектура машини фон-Неймана та Гарвардська архітектура. Їх переваги та недоліки. Стандартний цикл виконання команди.
2. Архітектура першого ІВМ-сумісного персонального комп'ютера. Поняття про шину розширення. Розвиток архітектури ІВМ-сумісного персонального комп'ютера.
3. Поняття про мікропроцесор. Закон Мура розвитку мікропроцесорної галузі. Розвиток мікропроцесорів фірми Intel.
4. Критичні обмежені ресурси персонального комп'ютера. Поняття про РnP-технологію.
5. Структура апаратного та програмного забезпечення сучасного персонального комп'ютера. Файлові системи сучасних операційних систем.

## АРХІТЕКТУРА ТА ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1. Архітектурне проектування. Структурування системи. Модель репозиторія. Модель клієнт-сервер. Модель абстрактної машини.
2. Проблемно-залежні архітектури. Моделі класів систем. Базові моделі.
3. Моделі розподілених систем. Багатопроцесорна архітектура. Архітектура клієнт-сервер. Архітектура розподілених об'єктів. Модель CORBA.
4. Об'єктно-орієнтоване проектування. Патерни проектування. Класифікація патернів проектування. Використання патернів у процесі об'єктно-орієнтованого проектування.
5. Рефакторинг: покращення існуючого коду. Рефакторинг з використання патернів проектування.

## ЛЮДИНО-МАШИННА ВЗАЄМОДІЯ

1. Людино-машинна взаємодія. Класифікація інтерфейсів користувача. Стили взаємодії з користувачем. Способи представлення даних.
2. Етапи розробки інтерфейсу користувача. Види документації до програмного забезпечення. Попереднє проектування. Проектування загальної структури, окремих блоків. Побудова прототипу. Версії. Тестування прототипу. Принципи та методи тестування.
3. Моделі кількісного аналізу інтерфейсів. Правила розрахунків за моделлю GOMS (KLM). Інформаційна та символна продуктивність інтерфейсу. Закони Фітса та Хіка. Кнопка безкінечного розміру та нульова дистанція.
4. Критерії якості інтерфейсу. Швидкість виконання роботи, її складові. Тривалість інтелектуальної роботи. Способи зменшення витрат часу на інтелектуальну діяльність. Тривалість фізичних дій та реакції системи.
5. Помилки користувачів. Типи та рівні помилок. Попередження помилок. Необхідність навчання користувачів роботі з інтерфейсом. Засоби навчання. «Зрозумілість системи». Ментальна модель та метафора. Аффорданс та стандарт.
6. Структура довідкової системи в інтерфейсі. Типи довідок. Представлення довідкових матеріалів. Принцип спіральності в довідковій системі.
7. Суб'єктивне задоволення користувача. Підвищення суб'єктивної швидкості роботи користувача з інтерфейсом.

## МОДЕЛЮВАННЯ ТА АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1. Загальні поняття теорії моделювання (об'єкт, модель, моделювання). Сутність та цілі моделювання. Класифікація моделей. Форми представлення моделей. Класифікація видів моделювання.
2. Моделювання бізнес-процесів. Загальні положення. Методологія IDEF0. Методологія DFD. Методологія IDEF3.
3. BPMN. Сфера застосування. Об'єкти потоку (події, дії, логічні оператори). З'єднуючі об'єкти (потоки керування, повідомлень, асоціації). Ролі. Артефакти.
4. UML. Діаграма варіантів використання. Актори. Взаємозв'язки між прецедентами. Розширення для бізнес моделювання. Документування варіантів використання.
5. Діаграма класів. Вимоги до зображення класів, атрибутів. Інтерфейс. Операції класу. Розширення UML для бізнес систем. Зв'язки (асоціація, узагальнення, наслідування, агрегація, композиція, залежність).
6. Діаграма кооперації. Об'єкти та зв'язки між ними. Повідомлення.
7. Діаграма послідовності. Повідомлення на діаграмі послідовності. Розгалуження потоку керування.
8. Діаграма станів. Стани. Переходи та події. Складні стани та їх складові. Історичні стани. Складні переходи та псевдостани.
9. Шаблони проектування.

## БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

1. Інформація. Особливості та властивості інформації. Цінність. Об'єктивне оцінювання кількості інформації. Інформаційна безпека. Категорії інформації з точки зору інформаційної безпеки (доступність, цілісність, конфіденційність, автентичність, апельованість). Комп'ютерна система як об'єкт захисту інформації. Система захисту інформації в комп'ютерних системах.
2. Загрози безпеці інформації в комп'ютерних системах. Класифікація загроз. Несанкціонований доступ до інформації. Несанкціонована модифікація структур. Шкідливі програми. Класифікація зловмисників.
3. Захист інформації в комп'ютерних системах від випадкових загроз. Складові. Дублювання. Технологія RAID. Рівні RAID (основні та комбіновані). Технологія JBOD. Підвищення надійності комп'ютерних систем. Створення відмовостійких комп'ютерних систем. Блокування помилкових операцій. Оптимізація взаємодії людини з комп'ютерною системою. Підходи до мінімізації втрат від аварій та стихійних лих.
4. Методи захисту від несанкціонованої зміни структури комп'ютерної системи. Захист від закладок під час розробки програм. Захист від вбудовування апаратних закладок. Розмежування доступу до обладнання. Протидія несанкціонованому підключенню приладів. Контролювання цілісності програмної структури в процесі використання.
5. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Система розмежування доступу до інформації. Захист програмних засобів від копіювання та дослідження.
6. Криптографічний захист інформації. Цілі та задачі. Загальні вимоги до методів та систем шифрування. Формальна модель та класифікація шифрів. Симетричні системи шифрування. Шифри перестановки, заміни або підстановки (моноалфавітні, гомофонічні, поліалфавітні, поліграмні). Гамування. Комбіновані шифри. DES стандарт.
7. Асиметричні криптографічні системи. Односторонні функції, односторонні функції з секретом. Процедура відкритого розповсюдження ключів Діффі-Хеллмана. Криптосистема RSA. Алгоритм шифрування Ель Гамала. Схеми на основі еліптичних кривих.

- Одночасне використання симетричних та асиметричних методів в одній криптосистемі. Способи підвищення стійкості шифрів.
8. Електронний цифровий підпис (ЕЦП). Принцип побудови та перевірки. ЕЦП на базі алгоритму DSA. Хеш-функції (дайджест) повідомлення. Односпрямовані хеш-функції на основі симетричних блочних алгоритмів. Алгоритм MD5. Алгоритм SHA. Арбітражні цифрові підписи.
  9. Безпека в відкритих мережах. Інфраструктура на основі криптографії з відкритими ключами. Цифрові сертифікати. Керування цифровими сертифікатами. Компоненти інфраструктури на основі криптографії з відкритими ключами та їх функції. Центр сертифікації. Центр реєстрації. Кінцеві користувачі. Мережевих довідник. Використання в програмних продуктах. Стандарти в сфері інфраструктури на основі криптографії з відкритими ключами. Керування ключами.
  10. Стеганографічний захист інформації. Загальні поняття. Математичні моделі стеганосистем. Цифрові водяні знаки. Основні методи та алгоритми вбудовування та знаходження водяних знаків. Види атак на інформаційні ресурси, що містять водяні знаки.

### ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

1. Локальні і глобальні мережі комп'ютерів. Топологія локальних мереж комп'ютерів.
2. Семирівнева мережна архітектура.
3. Методи доступу і протоколи передачі даних.
4. Види блокувань і керування блокуваннями. Обробка транзакцій.
5. Апаратне забезпечення локальних мереж.
6. Стандарти технології Ethernet.
7. Проектування локальної мережі. Загальні вимоги і критерії.
8. Вибір топології мережі і методу доступу. Вибір мережного апаратного забезпечення.
9. Мережеві операційні системи, настроювання та застосування, мережеві засоби та сервіси операційних систем
10. Розподілена обробка даних. Робота з базами даних в режимі мережі. Види блокувань, їх застосування
11. Робота в глобальній мережі Інтернет. Вибір та налаштування обладнання. Ефективне застосування пошукових систем
12. Безпека та таємність даних, засоби мережевої безпеки
13. Методологія проектування та створення корпоративної мережі
14. Засоби дослідження та тестування роботи мережі, усунення колізій
15. Бездротова передача даних, переваги та недоліки бездротових систем різних видів

## ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ:

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стенография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с., ил. описание.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стенография. – М.: «Солон-Пресс», 2002. – 272 с., ил.
3. Пилигрим А. Персональный компьютер: модернизация и ремонт: пер. с англ. – СПб.: ВНУ – Санкт-Петербург, 1999. – 528 с., ил.
4. Гук М. Аппаратные средства IBM PC. Энциклопедия, 2-е изд. – СПб.: Питер, 2002. – 928с., ил.
5. Авен О.И., Коган Я.А. Управление вычислительным процессом в ЭВМ. – М.: Энергия, 1978. – 240 с.
6. Роберт Т. Фатрелл, Дональд Ф. Шафер, Линда И. Шафер. Управление программными проектами. Достижение оптимального качества при минимуме затрат. Издательство: Вильямс, 2003 – 1136 с.
7. Леффингуэлл Дин, Уинриг Дон. Принципы работы с требованиями к программному обеспечению. Унифицированный подход.–М.:Издательский дом «Вильямс», 2002.– 432 с.
8. Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы. М.: Мир, 1976, 735с.
9. Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977, 724с.
10. Кнут Д. Искусство программирования для ЭВМ.Т. 3. Сортировка и поиск. М.: Мир, 1978.
11. Б.Лисков, Дж.Гатег. Использование абстракций и спецификаций при разработке программ. М.: Мир, 1989, 424с.
12. Агафонов В.Н. Данные в языках программирования: Абстракция и топология: Сб. статей /Пер. с англ. Под ред. В.Н.Агафонова.- М.: Мир, 1982.- 328с.
13. Агафонов В.Н. Требования и спецификации в разработке программ. (Сб. статей). М.: Мир, 1984, 344с.
14. Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. : Пер. с англ.: М.: Издательский дом "Вильямс", 2001.- 384с.: ил
15. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. /Пер. с англ. А.О. Слисенко. Под ред. Ю.В. Матиясевича.- М. :Мир, 1979.- 536с.
16. Вирт Н. Алгоритмы + структуры данных = программы: Пер. с англ.- М.: Мир, 1985.- 406с.
17. Мейер Б., Бодуэн К. Методы программирования. М.: Мир, 1982, Т. 1. 356с.
18. Мейер Б., Бодуэн К. Методы программирования. М.: Мир, 1982, Т. 2. 368с.
19. Сибуя М., Ямамото Т. Алгоритмы обработки данных. /Пер. с яп. Э.К. Николаевой. Под ред. В.В. Панферова.- М.: Мир, 1986.- 218с. :ил.
20. Иан Соммервил. Инженерия програмного обеспечения. 6-е издание.: Пер. с англ.- М.: Издательский дом “Вильямс”, 2002.- 624с.: ил.
21. Фаулер М. Архитектура корпоративних программных приложений. – Пер. с англ. – Издательский дом “Вильямс”, 2006.- 544с.: ил.
22. Джошуа Кериевски. Рефакторинг с использованием шаблонов.: Пер. с англ. – М.: ООО “И.Д. Вильямс”, 2006.- 400с.: ил.
23. Э. Фримен, Э. Фримен, К. Сьерра, Б. Бейтс. Паттерны проектирования.- СПб.: Питер, 2011.- 656с.: ил.
24. Фаулер М. Рефакторинг: улучшение существующего кода. – Пер. с англ. – СПб: Символ-Плюс, 2003.- 432с.: ил.
25. Бройдо В.Л., Ильина О.П. Архитектура ЭВМ и систем: Учебник для вузов. – СПб.: Питер, 2006.- 718с.: ил.

26. Гук М. Аппаратные интерфейсы ПК: Энциклопедия: Наиболее полное руководство.- Спб.: Питер, 2002.- 528с. :ил.
27. Гудман Дж Управление памятью для всех. -К. Диалектика 1996. - 528 с., ил.
28. Гук М. Аппаратные средства IBM PC. Энциклопедия, 2-е изд. - Спб.:Питер, 2002.- 928с.: ил.
29. Гук М. Дисковая подсистема ПК. - Спб.: Питер, 2001.- 336с., ил. - (Анатомия ПК).
30. Гук М. Процессоры Pentium II, Pentium PRO и просто Pentium: Архитектура. Интерфейс. Программирование. - Спб.: Питер, 1999.- 288с. :ил.
31. Гук М. Процессоры Intel: от 8086 до Pentium II: Архитектура. Интерфейс. Программирование. - Спб.: Питер, 1998.- 224с.
32. Гук М. Процессоры Pentium 4, Athlon и Duron. - Спб.: Питер, 2001.- 512с. :ил.- (Анатомия ПК).
33. Кузьмина О.О. Архітектура і програмне забезпечення ЕОМ: Навч. посіб.- Дніпропетровськ.: РВВ ДНУ, 2002,- 64с.
34. Хандецкий В.С. Архітектура комп'ютерів: Навч. посіб. /ДНУ. Ін-т довузівської підготовки та післядипломної освіти.- Дніпропетровськ: РВВ ДНУ, 2003.- 80с.
35. Олифер В. Г., Олифер Н. А. Сетевые операционные системы. — Спб.: Питер, 2001.
36. Олифер В. Г., Олифер Н. А. Новые технологии и оборудование IP-сетей. Спб.: БХВ-Санкт-Петербург, 2000.
37. Аннабел З. Дод. Мир телекоммуникаций. Обзор технологий и отрасли. — М.Г ЗАО «Олимп-Бизнес», 2002.
38. Танненбаум Э. Компьютерные сети. — Спб.: Питер, 2002.
39. Щербо В. К., Киреичев В. М., Самойленко С. И. Стандарты по локальным вычислительным сетям: Справочник / Под ред. С. И. Самойленко. — М.: Радио и связь, 1990.
40. Дженнингс Ф. Практическая передача данных: Модемы, сети и протоколы. Перев. с англ. — М.: Мир, 1989.
41. Блэк Ю. Сети ЭВМ: протоколы стандарты, интерфейсы / Перев. с англ» — М.:Мир, 1990.
42. Куинн Л., Рассел Р. Fast Ethernet. - ВНУ-Киев, 1998.
43. Джим Кох, Кен Дэвидсон. XML. Огромные возможности и легкость изучения.
44. Джеймс Бин. XML для проектировщиков. Повторное использование и интеграция.
45. Динар Дальви, Джо Грэй, Бипин Джоши, Фредрик Нормен, Фрэнсис Нортона, Энди Ольсен, Дж. Майкл Палермо, Кевин Уильямс. XML для разработчиков-профессионалов .NET.
46. Головач В.В. Дизайн пользовательского интерфейса, 146 с.
47. Раскин Д. Интерфейс: новые направления при проектировании компьютерных систем, Пер с англ., – Спб: Символ-Плюс, 2006. –272 с.
48. А.К. Гулятьев, В.А. Машин Проектирование и дизайн пользовательского интерфейса. – Спб.: КОРОНА принт, 2007. - 352с.
49. Крэг Ларман, Применение UML 2.0 и шаблонов проектирования (3-е издание). Вильямс 2006. – 496 с.
50. Фаулер, М. UML. Основы. Символ-Плюс, 2006. - 184 с.
51. Д.Марко и К.МакГоуэн "Методология структурного анализа и проектирования SADT" <http://www.interface.ru/home.asp?artId=1852>
52. Буч Г., Рамбо Дж., Джекобсон А. - UML. Руководство пользователя. М: ДМК-Пресс, 2007.- 496 с.
53. Завгородний В.И. Комплексная защита информации в компьютерных системах. – М:Логос, 2001. – 264 с.
54. Адигеев М.Г. Введение в криптографию. Метод. указания. Ростов на Дону, 2002.
55. Горячкв Г.А. Методы и средства защиты компьютерной информации. Метод. указания. – Спб.: ЛЭТИ, 2006



56. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб:Наука и техника,2004. – 321 с.
57. Куприянов А.И. Основы защиты информации. – М:Академія, 2006, -256 с.
58. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. – Фенікс, 2006. – 173 с.
59. Грибулин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.:СОЛОН-ПРЕСС, 2009, - 272 с.
60. Стеганография, цифровые водяные знаки и стеганоанализ: Монография. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. – М.: Вузовская книга, 2009, - 220 с.
61. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288с.