

## 1. Архітектура комп'ютерних систем

1. Аналогові та цифрові ЕОМ. Архітектура **фон Неймана** та Гарвардська архітектура. Багаторівнева організація обчислювальних систем. Архітектура процесора. Особливості RISC і CISC процесорів.
2. Представлення чисел в ЕОМ. Правила **Двійкової арифметики**. Формати з фіксованою і плаваючою крапкою (комою). Діапазон і точність представлених чисел.
3. Паралелізм на рівні команд (**конвеєри**). Приклад 5-ти стадійного конвеєра. Параметри ефективності конвеєра. Суперскалярна архітектура комп'ютерів. Приклад – процесор Intel Pentium. Сучасне поняття суперскалярної архітектури.

## 2. Операційні системи

1. **Типи ядер** операційних систем: монолітне, модульне, гібридне, мікроядро, наноядро, екзоядро. Приклади ОС з різними ядрами.
2. **Процеси і потоки**: означення, моделі, схеми багатопотоковості, опис процесів і потоків у системі. Приклади реалізації у різних ОС (Linux, Windows).
3. Стани потоків і **переходи між станами**, завдання і алгоритми планування процесів (потоків). Приклади реалізації у різних ОС (Linux, Windows).
4. **Керування пам'яттю**: завдання, методи розподілу пам'яті, віртуальна пам'ять. Сегментний і сторінковий розподіл пам'яті у процесорах x86.
5. Організація пристроїв введення-виведення. Контролер, драйвер, оброблення переривань. **Драйвери в Linux і Windows**.
6. **Файлові системи**: визначення, атрибути файлів, опис розміщення файлів на диску. Приклади файлових систем (FAT32, NTFS, ext2/3).
7. **Об'єкти ядер ОС**. М'ютекси, критичні секції, семафори, файлмепінги. Приклади для Linux та Windows.

## 3. Інформаційно-комунікаційні системи 1. Базы даних та інформаційні системи

1. Реляційна модель даних (**РМД**). Структуризація даних в РМД. Обмеження цілісності. Функціональні залежності в РМД. Декомпозиція відносин за функціональними залежностями.
2. Теоретико-множинні **операції реляційної алгебри**. Спеціальні операції реляційної алгебри. Пріоритет операцій реляційної алгебри.
3. **Аномалії виконання операцій** при некоректній схемі БД. Поняття нормалізації відношень. Типи нормальних форм
4. **Етапи проектування** реляційної бази даних. Модель сутність-зв'язок: основні поняття і властивості. Перетворення моделі сутність-зв'язок в реляційну схему БД.
5. **Мова SQL**. Типи даних. Команди категорій DDL і DML. З'єднання

таблиць. Агрегатні функції. Групування результатів запитів. Вкладені запити.

6. **Індексування даних.** Види індексів. Індеси типу В – дерева
7. **Транзакція** як механізм забезпечення несуперечності даних. Властивості транзакції
8. **Захист даних в БД** від несанкціонованого доступу. Основні механізми захисту в БД: автентифікація, керування доступом, реєстрація і аудит.
4. **Інформаційно-комунікаційні системи 2. Комп'ютерні мережі**
  1. Модель взаємодії **відкритих систем**. Завдання кожного з рівнів.
  2. **Канальний рівень моделі** взаємодії відкритих систем. Підрівні, їх завдання. Стандарти.
  3. **Логічна структуризація мереж**. Віртуальні локальні мережі. Алгоритм прозорого мосту. Алгоритм і протокол STP.
  4. **Маршрутизація** – завдання, принципи, протоколи.
  5. **Стек протоколів TCP/IP**. Протокол IP. Адресація. Протоколи UDP і TCP.
5. **Інформаційно-комунікаційні системи 3. Системи та мережі передачі інформації.**
  1. **Канали зв'язку та канали передавання**, основні поняття, визначення та характеристики.
  2. **Первинна мережа**, канали та тракти систем передачі.
  3. **Аналогові системи передачі**.
  4. **Цифрові системи передачі**.
  5. Механізм утворення **мовного сигналу**, його основні властивості.
  6. Види та **методи модуляції**.
  7. **Кодування** форми сигналу та джерела сигналу.
  8. Особливості кодування сигналів у **лінійних трактах** цифрових систем передачі.
  9. **Вокодери**: принцип дії, основні види.
  10. **Мобільний зв'язок**.
  11. Принципи багатоканальної передачі сигналів, **кодове розділення каналів**.
6. **Технології програмування**
  1. **Функції в C++**. Прототипи. Передача параметрів за замовчуванням. Перевантаження.
  2. Основні властивості **ООП**.
  3. Одиночне та множинне **успадкування**. Типи за специфікатором доступу.
  4. **Поліморфізм** та його реалізація в C++. Абстрактний клас. Віртуальні функції.
  5. Архітектурні шаблони **web-додатків**.
  6. Порівняльний аналіз **структурного та об'єктно-орієнтованого** підходів до програмування.

## 7. Захист інформації в інформаційно-комунікаційних системах 1. Захист програмного забезпечення та даних.

1. Основні види вразливостей програмного забезпечення. Вразливості WEB- додатків. **Міжнародні класифікатори** вразливостей.
2. Модель загроз програмного забезпечення. Етапи побудови моделі. Класифікація загроз за методикою **STRIDE**. Оцінка ризиків за методикою **DREAD**. Моделювання загроз за допомогою дерева атаки.
3. Загальні вимоги до механізму автентифікації додатків. Типи ідентифікаторів. **Вимоги до реалізації механізму автентифікації** за допомогою паролів, умов зберігання паролів. Особливості реалізації механізму автентифікації в WEB-додатках.
4. Структура файлів що виконуються. **Особливості ураження** файлів, що виконуються комп'ютерним вірусом. Типи комп'ютерних вірусів. Особливості поліморфних вірусів.
5. Зловмисне програмне забезпечення типу комп'ютерний черв'як і **троянський кінь**: структура, методи розповсюдження. Методи виявлення.
6. Програмно-апаратні засоби захисту додатків від несанкціонованого використання. Методи захисту програмного забезпечення від **зворотного аналізу**.
7. Організаційні і правові методи захисту додатків від **неліцензійного використання**.

## 8. Захист інформації в інформаційно-комунікаційних системах 2. Безпека операційних систем та ком'ютерних мереж.

1. **Модель загроз** для операційної системи. Типова архітектура комплексу засобів захисту операційних систем.
2. Склад і **архітектура засобів захисту ОС Windows**.
3. Склад і **архітектура засобів захисту ОС Linux**.
4. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (**НД ТЗІ**)
5. Стандарт **ISO 15408** (Common Criteria)
6. Загрози безпеці інформації у комп'ютерних мережах, віддалені атаки. Вразливості протоколів Інтернету (**IP, TCP, UDP, DNS**).
7. Безпека WWW: вразливості серверного і клієнтського ПЗ. **Атаки XSS**. Безпека CGI-застосувань, ін'єкції, методи захисту.
8. **Віртуальні приватні мережі (VPN)**. Сервіси віртуальних приватних мереж. Типи віртуальних приватних мереж. Протоколи.

## 9. Комплексні системи захисту інформації: проектування, впровадження, супровід.

1. Несанкціонований доступ (**НСД**) до інформації. Способи та види НСД.
2. **Політика безпеки**. Призначення і основні складові політики безпеки.
3. Джерела загроз, **модель загроз**, модель порушника. Категорії

порушників.

4. Ідентифікація та автентифікація (ІА). **Методи ІА.**
5. Система **нормативних документів України** із захисту інформації.
6. Класифікація інформації за режимом доступу та за правовим режимом. Види інформації, **захист якої гарантується державою.**
7. Класи і категорії автоматизованих інформаційних систем. Стандартні **функціональні профілі** захищеності інформації, що обробляється, від несанкціонованого доступу
8. Етапи побудови комплексної системи захисту інформації (**КСЗІ**). Зміст робіт, що виконуються на окремих етапах. Документи, що розробляються для кожного етапу створення КСЗІ.
9. Призначення і зміст робіт на етапі **обстеження об'єкту** інформаційної діяльності
10. **Оцінка ризиків** порушення інформаційної безпеки.
11. Види технічних **каналів витоку** інформації.
12. Види державної **експертизи** КСЗІ. Види атестації комплексу ТЗІ.
13. **Критерії оцінки** захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Види критеріїв, їх призначення. Рівні оцінок за критеріями.
14. Дискреційні моделі керування доступом. Модель **HRU**. Властивості моделі та теореми розв'язності задачі безпеки. Модель **TAM** та її властивості.
15. Модель **Take-Grant**. Формалізація санкціонованого отримання прав доступу та крадіжки прав доступу. Розширена модель Take-Grant. Правила де-юре та де-факто.
16. Моделі тематичного керування доступом. Модель решітки цінностей. Решітка **MLS**.
17. Моделі мандатного керування доступом. Властивості мандатного керування доступом. Модель **Белла-ла-Падули**. Основна теорема безпеки.
18. Проблеми мандатного керування доступом. Розвиток моделі Белла-ла-Падули: Z-система Мак-Ліна, модель **Low-Watermark**.
19. **Рольові моделі** керування доступом.
20. Моделі забезпечення цілісності даних (**Біба**, Кларка-Вілсона та похідні моделі).

## **10. Системи технічного захисту інформації**

1. Захист мовної інформації в системах телекомунікації.
2. Технічні канали витоку інформації.
3. Закладні пристрої.
4. Методи захисту мовної інформації в приміщенні.

## **11. Теорія інформації та кодування**

1. **Інформаційні характеристики** дискретних каналів зв'язку.

## 12. Симетрична криптографія. Асиметричні криптографічні системи та протоколи

1. Основні поняття криптології. Теорія зв'язку в секретних системах **Шеннона**.
2. Сучасні **блокові** шифратори.
3. **Регістри** зсуву з лінійним оберненим зв'язком та їх застосування у криптографії.
4. Важкооборотні функції, схема відкритого розповсюдження ключів Діффі-Хеллмана, система шифрування **RSA**.
5. **Функції хешування**, алгоритми автентифікації та цифрового підпису

## М. Математика

1. Алгебра матриць (лінійні операції, множення, обернена та алгоритми її відшукування). Матриця лінійного оператора та її перетворення при заміні базису. **Жорданова** форма матриці.
2. Визначники  $n$ -го порядку, їх властивості. Техніка обчислення **визначників**.
3. Формули **Крамера** для розв'язків системи лінійних алгебричних рівнянь. Метод Гаусса.
4. Системи лінійних алгебричних рівнянь. **Теорема Кронекера – Капеллі**. Фундаментальна система розв'язків.
5. Власні вектори та власні значення матриці. Алгоритм їх відшукування. Властивості **власних векторів** та власних значень симетричних матриць.
6. Векторна алгебра. **Скалярний, векторний, мішаний** добуток векторів та їх властивості.
7. Аналітична геометрія: рівняння основних **геометричних об'єктів** на площині та у просторі.
8. Поняття послідовності. Збіжні та розбіжні послідовності, границя збіжної послідовності. **Критерій Коші** існування границі. Нескінченно малі послідовності та їх основні властивості.
9. Означення границі функції у точці мовою послідовностей (за **Гейне**) та мовою нерівностей (за Коші). Критерій існування границі мовою односторонніх границь. Неперервні функції, класифікація точок розриву неперервної функції.
10. **Граничний перехід** у сумі, добутку, частці та у нерівностях для функцій. Невизначеності, їх види та способи розкриття. Порівняння функцій в околі точки. Таблиця еквівалентних нескінченно малих при  $x \rightarrow 0$  функцій.
11. Поняття **похідної** та **диференціалу** функції. Інваріантність першого диференціалу та його застосування до наближених обчислень. Похідні та диференціали вищих порядків.

12. Формула **Ньютона – Лейбніца**. Застосування визначеного інтеграла для знаходження геометричних та фізичних величин (площі, об'ємів, центрів мас, моментів інерції тощо).
13. Поняття **числового ряду** та його суми. Ознаки збіжності числових рядів.
14. Поняття функціонального ряду та його області збіжності. Вигляд області збіжності степеневому ряду. Степеневий **ряд Тейлора**.
15. **Формула Тейлора** та ряди Тейлора для найважливіших елементарних функцій.
16. Ряд Фур'є періодичної функції. Дійсна та комплексна форма ряду Фур'є. Інтеграл та перетворення **Фур'є**.
17. Диференційовність функції декількох змінних. Часткові похідні та диференціал. Вигляд **диференціалу  $n$ -го порядку** для функції декількох змінних.
18. Локальні та глобальні **екстремуми** функції декількох змінних. Алгоритм їх відшукування.
19. Кратні інтеграли. **Теорема Фубіні** (Зведення кратних інтегралів до повторних). Заміна змінних у кратному інтегралі.
20. Криволінійні та **поверхневі інтеграли** 1-го і 2-го роду: означення і властивості, способи обчислення.
21. Основні інтегральні формули аналізу (**Гріна** на площині, **Остроградського – Гаусса** та **Стокса** у просторі).
22. Поняття імовірнісного простору. Геометрична та класична модель. **Модель Бернуллі**.
23. Поняття дискретної та неперервної випадкової величини. Основні дискретні та неперервні розподіли (**Бернуллі**, **Пуассона**, геометричний, експоненціальний, **Коші**, **гауссовий**). Їх числові характеристики – математичне очікування, дисперсія, моменти.
24. Теорема Чебишева про закон великих чисел. Інтегральна гранична теорема **Муавра-Лапласа**.
25. **Інтервальне оцінювання**. Оцінка середнього та дисперсії гауссового розподілу.