МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

15.03.2025

Захист розподілених баз даних та інформаційних систем

Електронне видання

Методичні вказівки до організації самостійної роботи студентів (СРС)
для студентів всіх форм навчання освітнього ступеня «Бакалавр» галузі знань
12 Інформаційні технології

Дрогобич
ДВНЗ «ДонНТУ»
2025

УДК 004.75.056.5:004.775](072)

З - 38

Захист розподілених баз даних та інформаційних систем. Методичні вказівки до організації самостійної роботи студентів (СРС) для студентів всіх форм навчання освітнього ступеня «Бакалавр» галузі знань 12 Інформаційні технології. [Електронне видання] / уклад.: Я.Ю. Дорогий. – Дрогобич : ДВНЗ «ДонНТУ», 2025. – 41 с.

Методичні вказівки призначені для студентів всіх форм навчання освітнього ступеня «Бакалавр» галузі знань 12 Інформаційні технології. В посібнику наведена тематика СРС, теоретичні відомості, завдання для виконання робіт, список літератури.

Укладач Ярослав ДОРОГИЙ, д.т.н., проф., в.о. зав. каф. ПМІ

Відповідальний редактор Ярослав ДОРОГИЙ, д.т.н., проф., в.о. зав. каф. ПМІ

Рецензент Василь ЦУРКАН, доцент, к. т. н., доцент спеціальної кафедри №5 ІСЗЗІ КПІ ім. Ігоря Сікорсь-кого

Затверджено навчально-методичним відділом ДонНТУ,
протокол №5 від 25.03.2025 р.
Розглянуто на засіданні кафедри прикладної математики та інформатики
протокол № 3 від 18.03.2025 р.

ЗМІСТ

ВСТУП

Розподіл годин на дисципліну (із загальних 180 годин на дисципліну, 32 виділяється на лабораторні роботи та 116 — на самостійну роботу студентів) визначає основне навантаження із засвоєння цієї дисципліни, а саме на практичну роботу студентів..

Практична суть освіти полягає в тому, що завданням викладача є не стільки передача певних знань студенту, скільки вміння навчити студента, маючи деякий мінімальний обсяг інформації, методам збільшення цього обсягу як на практичних заняттях під керівництвом викладача, так і вдома, в бібліотеці тощо.

Лише постійне самостійне навчання дає можливість наблизитись до глибин знань певної галузі, оволодіти достатньою сумою знань і вмінь, які б дали змогу почувати себе професіоналом.

1 МЕТА ТА ЗАВДАННЯ ДИСЦИПЛІНИ

Навчальна дисципліна «Захист розподілених баз даних та інформаційних систем» спрямована на забезпечення студентів необхідними знаннями та практичними навичками у галузі захисту інформації, що обробляється в розподілених інформаційних системах. Ця інформація включає в себе технічні та організаційні механізми захисту, що становлять невід'ємну частину розподілених інформаційних систем та баз даних. Переважно, навчальна дисципліна відповідає нормативним вимогам освітньо-професійної програми.

Мета навчальної дисципліни «Захист розподілених баз даних та інформаційних систем» полягає у сприянні формуванню когнітивних, афективних та моторних компетентностей в контексті вивчення та розуміння принципів організації та реалізації віддаленої обробки даних з використанням технології "клієнт-сервер", систем управління базами даних (СУБД), які підтримують цю технологію, захищених ІКС на базі технологій Cisco. Дисципліна націлена на розвиток теоретичних та практичних навичок студентів у сфері використання відповідного алгоритмічного та програмного забезпечення, а також СУБД (зокрема, на прикладі СУБД Oracle), оволодіння принципами створення та ведення баз даних і способами забезпечення інформаційної безпеки засобами систем управління базами даних, принципами створення та підтримки захищених ІКС на базі технологій Cisco; створення необхідного комплексу навичок і знань, необхідних для вирішення задачі побудови захищеної розподіленої системи управління базою даних на базі Oracle та ІКС на базі технологій Cisco. Крім того, вона сприяє набуттю студентами відповідних компетентностей, які можна успішно використовувати у професійній діяльності.

Компетентності, які досягаються при вивченні дисциплін:

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК02. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК05.Здатність вчитися і оволодівати сучасними знаннями.

ЗК08. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ФК04. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

ФК10. Здатність виконувати моніторинг інформаційних, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Програмні результати навчання за дисципліною наступні:

– ПРН01. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

– ПРН02. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

– ПРН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійний діяльності.

– ПРН04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

– ПРН05. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у

професійний діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

– ПРН06. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

– ПРН09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

– ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

– ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

– ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

– ПРН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

– ПРН15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

– ПРН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

– ПРН2l. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дії з інформацією в

інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

В результаті вивчення дисципліни студенти повинні

ЗНАТИ:

– теоретичні основи і понятійний апарату розподілених баз даних та інформаційних систем;

– принципи створення та ведення розподілених баз даних і способи забезпечення інформаційної безпеки засобами систем управління базами даних;

– принципи побудови захищеної розподіленої системи управління базою даних на базі Oracle.

ВМІТИ:

– застосовувати отримані навики самостійного вивчення навчальної та наукової літератури, володіти понятійним апаратом;

– конфігурувати та використовувати для розв’язання задач РБД інструментальні засоби СУБД Oracle;

– проектувати та реалізовувати за допомогою засобів СУБД Oracle бази даних;

– організовувати роботу у режимі “клієнт-сервер” з використанням відповідного інструментарію – запитів, представлень;

– використовувати мову PL/SQL;

– розробляти програмні застосунки за допомогою Oracle APEX.

2 ВИДИ СРС

СРС може здійснюватись за допомогою:

– запам’ятовування певної інформації через опрацювання лекцій;

– активної роботи під час практичних та лабораторних занять;

– роботи над конспектами лекцій, планами практичних занять;

– опрацювання літературних джерел (самостійного конспектування вивченого матеріалу, рефератування окремих тем);

– роботи з каталогами звичайних і електронних бібліотек, інформаційно-пошуковими сервісами Internet;

– вивчення навчального матеріалу за підручниками, навчальними посібниками, практикумами тощо;

– опрацювання окремих тем матеріалу за першоджерелами, науковою і спеціальною літературою;

– підготовки доповідей, рефератів, презентацій за темами курсу;

– самотестування.

СРС під час лекції. Належне ведення конспекту під час лекції сприяє більш уважному засвоєнню нового матеріалу, збереженню необхідної інформації та дає студенту змогу в подальшому проаналізувати її. За умови класичного подання лекційного матеріалу засвоюється приблизно 20 % інформації. При викладанні дисципліни «Захист розподілених баз даних та інформаційних систем» за допомогою візуального відтворення деяких аспектів налаштування бази даних Oracle на лекціях показник засвоювання зростає до 40%.

Робота над конспектами лекцій, планами практичних занять. При опрацюванні матеріалу лекції слід зіставити законспектований матеріал з планом практичного заняття, що міститься у методичних матеріалах для практичних занять. Якщо у конспекті відсутній матеріал з окремих питань лекції або недостатньо розкриті деякі питання практичного заняття, або винесені на самостійне опрацювання, студент повинен звернутися до

рекомендованих підручників, навчальних посібників і відповідних методичних матеріалів. Підготовку практичного заняття з дисципліни слід здійснювати з використанням ПК з встановленим на ньому програмним забезпеченням Virtual Box. Також потрібно активно використовувати довідкові мережі операційної системи Linux та СУБД Oracle, за допомогою якої можна отримати відповіді стосовно використання різних команд, їх синтаксису і т.п.

Робота з літературою. Працювати з підручниками, навчальними посібниками, методичними вказівками, практикумами, науковою і спеціальною літературою незалежно від типу їх носія (паперового чи електронного) необхідно таким чином, щоб отримати максимум теоретичних знань і навичок. Для самостійного поглибленого вивчення навчального матеріалу студенту слід створити свій список літератури для опрацювання, джерела якого можуть і не бути зазначеними в якості основної чи додаткової літератури.

Робота з Internet. Сервіси мережі Internet надають унікальні можливості знаходження літературних джерел у географічно віддалених фондах та архівах, а також шляхом участі у мережевих конференціях, де можна отримати відповіді та поради щодо питань з розшукуваної інформації. Для пошуку інформації слід скористатись пошуковими системами.

Пошукові системи є складними інформаційно-довідковими системами, що автоматично генеруються на основі даних, які збираються мережевими програмами-роботами по всьому Internet, і дають у відповідь на запит користувача посилання на різні Internet-ресурси. Запит здійснюється за певною процедурою (певною мовою), яка може відрізнятися в різних системах, проте в спрощеному вигляді вона зводиться до введення в спеціальному полі певного виразу пошуку, що складається з ключових слів та деяких операторів мови запитів.

До загальних положень мов запитів належать:

− ключові слова можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або ж вводити відразу декілька слів, розділяючи їх пробілами або комами. Регістр не має значення.

− режим пошуку “AND” (“І”) означає, що будуть знайдені тільки ті дані, де зустрічається кожне з ключових слів.

− при використанні режиму “OR” (“АБО”) результатом пошуку будуть всі дані, де зустрічається хоча б одне ключове слово.

− використання знаків «+» і «-» перед ключовим словом. Щоб виключити документи, де зустрічається певне слово, поставте перед ним «-». І навпаки, щоб певне слово обов’язково було присутнє в документі, поставте перед ним «+». Зверніть увагу на те, що між знаком і словом не повинно бути пропуску. Наприклад: “+таблиці -Excell”.

− за замовчуванням програма шукає всі дані, в яких зустрічається введене слово. Наприклад, при запиті “редактор” будуть знайдені слова “редактор”, “текстовий”, “графічний”, “газети”, “головний” і багато інших. Знак оклику перед або після ключового слова означає, що будуть знайдені тільки слова точно відповідні запиту (наприклад, “текстовий! редактор!”).

Також корисно пам’ятати і використовувати при пошуку такі прийоми:

− якщо потрібно шукати словосполучення, вкладіть його в лапки;

− якщо запит вводиться малими літерами, будуть знайдені всі варіанти його написання; якщо при введенні вказана хоча б одна прописна літера, то система шукатиме тільки такий варіант;

− якщо потрібно знайти не текст, а зображення, то можна скористатися словом image. Наприклад, image: алгоритм дасть список сторінок із зображенням алгоритмів;

− якщо ключове слово, що шукається, зустрічається в різних контекстах, можна виключити слова з непотрібним контекстом. Наприклад, вказати аргумент пошуку +ОС +Налаштування +Linux++ -Windows.

− використання синонімів може збільшити кількість знайдених сторінок.

Велику популярність мають різні тематичні форуми, на яких користувач може поставити конкретне питання і отримати відповідь від інших членів форуму.

Самостійна робота має такі складові і форми її оцінювання:

− підготовка та аудиторна робота під час практичних і лабораторних занять, результати якої оцінюються під час поточного контролю;

− виконання самостійних робіт у формі підготовки усних доповідей у вигляді презентацій та домашніх контрольних робіт;

− опрацювання програмного матеріалу зі змістового модуля та оцінка результатів під час проміжного контролю;

− виконання МКР або ДКР (за наявності відповідного навантаження за дисципліною).

3 ТЕМАТИКА СРС

3.1 Загальні відомості

Програма вивчення дисципліни «Захист розподілених баз даних та інформаційних систем» складається з таких розділів: «Мета, задачі, зміст курсу. Основні визначення», «Архітектура розподілених баз даних та інформаційних систем», «Архітектура СУБД Oracle», «Автентифікація та авторизація в СУБД Oracle», «Захист та шифрування даних в СУБД Oracle», «Моніторинг та аудит безпеки в СУБД Oracle», «Резервне копіювання та відновлення СУБД Oracle», «Робота з SQL», «Мова програмування PL/SQL», «Розробка програмних застосунків в Oracle APEX».

В якості самостійної роботи студентами пропонується:

- підготувати реферат за обраною темою;
- створити презентацію за обраною темою та підготувати доповідь.

3.2 Тематика СРС

Тема 1. Мета, задачі, зміст курсу. Основні визначення.

1. Мета, задачі та зміст курсу. Опис мети курсу та основних задач. Визначення основних концепцій та тем, які будуть розглядатися протягом курсу: захист розподілених баз даних, захист інформаційних систем, шифрування, автентифікація та авторизація в середовищі СУБД Oracle.

2. Основні визначення у сфері захисту розподілених баз даних. Розгляд ключових термінів та понять: конфіденційність, цілісність та доступність даних у контексті розподілених систем, загрози та вразливості в базах даних. Визначення поняття "розподілена база даних" та "інформаційна система".

3. Розподілені бази даних та їх характеристика. Огляд основних характеристик розподілених баз даних. Принципи їх роботи, переваги та

недоліки. Порівняння з централізованими базами даних. Особливості використання СУБД Oracle в розподілених системах.

4. Основні загрози та ризики для безпеки розподілених баз даних. Аналіз основних загроз і ризиків для безпеки інформації в розподілених системах, зокрема в СУБД Oracle. Ризики, пов'язані з несанкціонованим доступом, порушенням цілісності даних, витоками інформації.

5. Принципи безпеки в розподілених інформаційних системах. Визначення основних принципів безпеки в розподілених системах. Методи захисту даних, включаючи шифрування, контроль доступу, резервне копіювання та відновлення.

6. Сучасні підходи до захисту даних в Oracle. Огляд методів захисту даних у СУБД Oracle: використання Transparent Data Encryption, механізмів автентифікації, управління правами доступу, аудит безпеки, захист від SQL-ін'єкцій.

Питання для самоперевірки з теми

1. Які основні задачі ставляться перед студентами в курсі "Захист розподілених баз даних та інформаційних систем"?

2. Що розуміється під термінами "конфіденційність", "цілісність" та "доступність" даних у контексті розподілених баз даних? Як ці принципи застосовуються в СУБД Oracle?

3. Які основні загрози і вразливості для безпеки даних існують в розподілених базах даних? Як вони можуть впливати на СУБД Oracle?

4. Як визначаються основні принципи безпеки в розподілених інформаційних системах? Які методи захисту даних застосовуються для забезпечення цих принципів у СУБД Oracle?

5. Чим відрізняються розподілені бази даних від централізованих? Які особливості захисту даних у розподілених системах та як їх реалізує СУБД Oracle?

Тема 2. Архітектура розподілених баз даних та інформаційних систем.

1. Основні компоненти архітектури розподілених баз даних. Опис основних елементів архітектури розподілених баз даних: сервери, клієнти, мережеві компоненти. Огляд ролей кожного елемента в забезпеченні безпеки та ефективності роботи системи.

2. Типи архітектур розподілених баз даних. Розгляд різних типів архітектур розподілених баз даних: однорівнева, багаторівнева, клієнт-серверна архітектура. Аналіз їх переваг і недоліків з точки зору безпеки та продуктивності.

3. Моделі даних в розподілених системах. Огляд моделей даних, що використовуються в розподілених базах даних: реляційна, об'єктно-орієнтована, документно-орієнтована. Особливості моделювання даних в розподілених системах для забезпечення безпеки.

4. Комунікація між компонентами в розподілених базах даних. Опис способів комунікації між компонентами системи (сервери, клієнти, вузли). Розгляд важливих аспектів, таких як шифрування даних, захист від несанкціонованого доступу та вразливості в мережевих комунікаціях.

5. Механізми відмовостійкості та балансування навантаження в розподілених системах. Огляд методів забезпечення високої доступності та відмовостійкості в архітектурі розподілених баз даних: використання кластерів, реплікація даних, балансування навантаження. Оцінка їх впливу на безпеку та надійність систем.

6. Безпека архітектури розподілених інформаційних систем. Розгляд специфічних загроз безпеки, які виникають у розподілених інформаційних системах: атаки на мережу, несанкціонований доступ до даних, атакування вузлів. Методи захисту та автентифікація користувачів у розподілених середовищах.

7. Роль СУБД Oracle в архітектурі розподілених баз даних. Огляд можливостей і функціональних характеристик СУБД Oracle для побудови

безпечних і масштабованих розподілених баз даних. Використання технологій Oracle для забезпечення безпеки та високої доступності.

Питання для самоперевірки з теми

1. Які основні компоненти складають архітектуру розподілених баз даних? Як кожен з цих компонентів забезпечує ефективність роботи системи?

2. Які основні типи архітектур розподілених баз даних існують? Які їх переваги та недоліки з точки зору безпеки та продуктивності?

3. Які моделі даних використовуються в розподілених системах, і як вони впливають на безпеку даних?

4. Які способи комунікації між компонентами в розподілених базах даних існують, і як забезпечується їх безпека?

5. Як механізми відмовостійкості та балансування навантаження впливають на надійність та безпеку розподілених інформаційних систем?

6. Які основні загрози безпеки виникають в архітектурах розподілених баз даних, і які методи захисту можуть бути застосовані для їх усунення?

7. Як СУБД Oracle підтримує архітектуру розподілених баз даних і які функції вона надає для забезпечення безпеки та високої доступності?

Тема 3. Архітектура СУБД Oracle.

1. Основні компоненти архітектури СУБД Oracle. Опис основних компонентів архітектури Oracle: фізичні та логічні структури бази даних, процеси, пам'ять та взаємодія між ними. Розгляд ролі кожного компонента в забезпеченні надійності та безпеки системи.

2. Архітектура пам'яті в Oracle. Розгляд основних елементів пам'яті в СУБД Oracle: System Global Area (SGA), Program Global Area (PGA). Вивчення їх ролі у зберіганні даних, буферизації та обробці запитів.

3. Процеси СУБД Oracle. Опис основних процесів, які працюють в Oracle: фонові процеси, наприклад, DBWn (Database Writer), LGWR (Log

Writer), CKPT (Checkpoint), PMON (Process Monitor). Їхня роль у забезпеченні стабільної роботи бази даних і підтримці її цілісності.

Питання для самоперевірки з теми

1. Які основні компоненти складають архітектуру СУБД Oracle? Як вони взаємодіють для забезпечення стабільної роботи бази даних?
2. Що таке System Global Area (SGA) та Program Global Area (PGA) в СУБД Oracle, і яка їх роль в управлінні пам'яттю?
3. Які процеси працюють у СУБД Oracle для підтримки її функціонування? Охарактеризуйте основні фонові процеси, такі як DBWn, LGWR, CKPT, PMON.
4. Яка роль процесу DBWn (Database Writer) в архітектурі СУБД Oracle і як він взаємодіє з іншими процесами?
5. Як працює механізм управління пам'яттю в СУБД Oracle, і яка роль кожного з компонентів пам'яті (SGA і PGA) у забезпеченні ефективної роботи системи?
6. Які основні функції виконує процес LGWR (Log Writer) в СУБД Oracle, і як він забезпечує цілісність бази даних?
7. Як взаємодіють процеси PMON та CKPT у забезпеченні надійності та відновлення бази даних в Oracle?

Тема 4. Автентифікація та авторизація в СУБД Oracle.

1. Основи автентифікації в СУБД Oracle. Опис механізмів автентифікації в Oracle: процес ідентифікації користувача та перевірки його особи. Розгляд різних методів автентифікації: локальна автентифікація, автентифікація через мережу, а також використання зовнішніх механізмів (наприклад, LDAP).

2. Методи автентифікації в Oracle. Розгляд методів автентифікації в Oracle: автентифікація за допомогою пароля, сертифікатів, інтегрованої

автентифікації через операційну систему (OS authentication). Опис протоколів та стандартів, що використовуються для забезпечення безпеки автентифікації.

3. Основи авторизації в СУБД Oracle. Опис принципів авторизації в Oracle: що таке ролі, привілеї та їх взаємодія. Як надаються права доступу до об'єктів бази даних на різних рівнях (система, схема, таблиця).

4. Типи прав доступу та привілеї в Oracle. Огляд типів прав доступу, які можуть бути надані в СУБД Oracle: системні привілеї, об'єктні привілеї та рольові привілеї. Визначення ролей у СУБД та їх використання для управління доступом.

5. Ролі та групи користувачів у СУБД Oracle. Опис ролей в Oracle: що таке роль користувача і як її призначити для групи користувачів. Використання попередньо визначених та користувацьких ролей для зручного управління доступом.

6. Методи контролю доступу в Oracle. Рівні доступу та моделі управління. Огляд моделей управління доступом в Oracle: DAC (Discretionary Access Control), MAC (Mandatory Access Control) та RBAC (Role-Based Access Control). Як ці моделі застосовуються в управлінні доступом до ресурсів бази даних.

Питання для самоперевірки з теми

1. Що таке автентифікація в СУБД Oracle і чому вона є важливою для безпеки бази даних?

2. Які методи автентифікації підтримує СУБД Oracle? Поясніть, у чому полягає різниця між локальною автентифікацією та автентифікацією через мережу.

3. Які переваги і недоліки має використання сертифікатів для автентифікації в Oracle?

4. Що таке авторизація в СУБД Oracle і які основні принципи авторизації використовуються для контролю доступу до бази даних?

5. Які типи прав доступу існують в Oracle? Як відрізняються системні, об'єктні та рольові привілеї?

6. Як створюються і призначаються ролі в Oracle? Яке їх значення для управління доступом до ресурсів бази даних?

7. Що таке об'єктні привілеї в Oracle і як вони застосовуються для доступу до таблиць та інших об'єктів бази даних?

8. Як система ролей і привілеїв в Oracle допомагає забезпечити гнучкий контроль доступу в базі даних?

9. Що таке моделі управління доступом DAC, MAC та RBAC в СУБД Oracle? Як вони відрізняються і які з них застосовуються в Oracle?

Тема 5. Захист та шифрування даних в СУБД Oracle.

1. Основи захисту даних в СУБД Oracle. Опис принципів захисту даних в СУБД Oracle: конфіденційність, цілісність та доступність даних. Розгляд основних механізмів захисту, таких як контроль доступу, автентифікація, авторизація та аудит.

2. Шифрування даних в СУБД Oracle: концепції та принципи. Огляд основних методів шифрування даних в Oracle: шифрування на рівні стовпців (Column-Level Encryption) і шифрування на рівні таблиць (Table-Level Encryption). Розгляд принципів шифрування та ключових аспектів захисту даних.

3. Transparent Data Encryption (TDE) в Oracle. Опис технології Transparent Data Encryption (TDE), яка забезпечує шифрування даних на рівні файлової системи. Як TDE захищає дані в базах даних Oracle і що таке шифрування для резервних копій даних.

4. Управління ключами шифрування в Oracle. Розгляд механізмів управління ключами шифрування в Oracle: створення та обробка ключів, захист ключів, використання Oracle Key Vault. Розгляд різних підходів до керування ключами шифрування для забезпечення безпеки даних.

5. Шифрування в транзиті: SSL/TLS в СУБД Oracle. Огляд використання шифрування для захисту даних під час передачі по мережі. Як SSL/TLS протоколи використовуються для захисту даних, що передаються між клієнтами та сервером Oracle.

6. Механізми автентифікації та шифрування паролів в Oracle. Опис технологій захисту паролів користувачів в Oracle: використання хешування паролів, автентифікація за допомогою сертифікатів. Як ці методи захищають дані від несанкціонованого доступу.

7. Використання Virtual Private Database (VPD) для захисту даних в Oracle. Розгляд технології Virtual Private Database (VPD) для забезпечення доступу до даних на основі політик безпеки. Як VPD допомагає захищати дані від несанкціонованого доступу на рівні запитів.

8. Захист даних у хмарі з Oracle. Огляд методів шифрування та захисту даних в хмарних рішеннях Oracle, таких як Oracle Cloud Infrastructure (OCI). Як використовуються технології шифрування для забезпечення конфіденційності даних в хмарі.

Питання для самоперевірки з теми

1. Що таке принципи захисту даних в СУБД Oracle, і як вони забезпечуються?

2. Які основні методи шифрування даних існують в Oracle, і чим вони відрізняються?

3. Що таке Transparent Data Encryption (TDE), і як ця технологія забезпечує захист даних в СУБД Oracle?

4. Які компоненти входять до складу TDE в Oracle, і як вони взаємодіють для захисту даних?

5. Як здійснюється управління ключами шифрування в Oracle? Які інструменти підтримує СУБД для керування ключами?

6. Що таке Oracle Key Vault і як він допомагає в управлінні ключами шифрування?

7. Які переваги надає шифрування на рівні стовпців і таблиць у СУБД Oracle?

8. Як забезпечується захист даних під час їх передачі в мережі за допомогою SSL/TLS в Oracle?

9. Що таке SSL/TLS, і як він використовується для шифрування даних в Oracle?

10. Як відбувається шифрування паролів користувачів у СУБД Oracle? Які механізми для цього використовуються?

11. Що таке Virtual Private Database (VPD), і як ця технологія допомагає захищати дані в Oracle?

12. Як захищаються дані в хмарі при використанні Oracle Cloud Infrastructure (OCI)? Які технології шифрування застосовуються для цього?

Тема 6. Моніторинг та аудит безпеки в СУБД Oracle.

1. Основи моніторингу та аудиту безпеки в СУБД Oracle. Огляд принципів моніторингу та аудиту безпеки в Oracle. Розгляд важливості моніторингу безпеки для виявлення потенційних загроз і вразливостей. Опис основних завдань аудиту безпеки.

2. Інструменти моніторингу безпеки в Oracle. Опис інструментів, які використовуються для моніторингу безпеки в Oracle: Oracle Enterprise Manager, Oracle Audit Vault, Oracle Data Safe. Як ці інструменти допомагають забезпечити безпеку баз даних.

3. Аудит подій в СУБД Oracle. Розгляд механізмів аудиту подій у СУБД Oracle: що таке аудит подій, які операції та дії підлягають аудиту, як налаштовуються журнали аудиту для відстеження важливих дій користувачів і адміністраторів.

4. Налаштування аудиту в Oracle. Опис процесу налаштування аудиту в Oracle: використання параметрів AUDIT_TRAIL, створення політик аудиту для різних типів подій. Як налаштувати аудит для моніторингу доступу до чутливих даних.

5. Моніторинг доступу та змін у даних. Огляд методів моніторингу доступу до даних та змін у таблицях і об'єктах бази даних. Використання тригерів і механізмів журналювання для відстеження змін в даних.

6. Аудит безпеки за допомогою Oracle Audit Vault. Розгляд функціональних можливостей Oracle Audit Vault для забезпечення централізованого аудиту та моніторингу. Як забезпечується збір і зберігання журналів аудиту з різних джерел і база даних для подальшого аналізу.

7. Виявлення та аналіз аномальної поведінки в СУБД Oracle. Опис технологій для виявлення аномальної поведінки та потенційних загроз в Oracle, зокрема з використанням Oracle Data Safe для виявлення незвичних доступів або змін у базі даних.

8. Механізми захисту журналів аудиту в Oracle. Огляд методів захисту журналів аудиту від несанкціонованого доступу та модифікації. Розгляд засобів шифрування та обмеження доступу до файлів журналу.

9. Аудит доступу до об'єктів бази даних в Oracle. Аналіз механізмів аудиту доступу до об'єктів бази даних, таких як таблиці, індекси, схеми. Як налаштовується аудит для виявлення несанкціонованих змін або спроб доступу до чутливих даних.

10. Інтеграція моніторингу та аудиту з іншими засобами безпеки. Розгляд інтеграції моніторингу та аудиту безпеки Oracle з іншими інструментами безпеки в корпоративному середовищі. Як поєднати ці механізми з системами управління безпекою та виявлення загроз.

Питання для самоперевірки з теми

1. Що таке моніторинг безпеки в СУБД Oracle, і чому він важливий для забезпечення захисту бази даних?

2. Які основні інструменти моніторингу безпеки в Oracle? Як вони допомагають виявляти потенційні загрози?

3. Що таке Oracle Audit Vault, і які функції цей інструмент надає для централізованого аудиту та моніторингу?

4. Які події в СУБД Oracle підлягають аудиту, і як налаштовується аудит для різних операцій?

5. Як налаштувати параметр AUDIT_TRAIL в Oracle для ведення журналів аудиту?

6. Що таке Oracle Data Safe, і як цей інструмент допомагає моніторити доступ до чутливих даних?

7. Як здійснюється моніторинг змін у даних бази даних в Oracle? Які механізми для цього використовуються?

8. Яким чином тригери можуть бути використані для моніторингу змін у таблицях бази даних в Oracle?

9. Як налаштовується аудит доступу до об'єктів бази даних в Oracle (таблиці, індекси, схеми)?

10. Що таке аномальна поведінка користувачів, і як Oracle допомагає виявляти таку поведінку в базі даних?

11. Які методи використовуються для захисту журналів аудиту в Oracle? Як гарантується, що журнали не будуть змінені?

12. Що таке журнал аудиту, і яку інформацію він містить в контексті безпеки СУБД Oracle?

13. Як здійснюється інтеграція моніторингу безпеки Oracle з іншими інструментами управління безпекою в організації?

14. Як забезпечити безпеку журналів аудиту в Oracle, і чому це важливо для забезпечення цілісності даних?

15. Що таке політики аудиту в Oracle, і як вони налаштовуються для забезпечення належного контролю доступу до даних?

Тема 7. Резервне копіювання та відновлення СУБД Oracle.

1. Основи резервного копіювання та відновлення в СУБД Oracle. Опис важливості процесу резервного копіювання для забезпечення безпеки даних. Основні стратегії резервного копіювання та відновлення в Oracle, а також їх роль у збереженні цілісності та доступності даних.

2. Типи резервних копій в Oracle. Огляд різних типів резервних копій, які підтримуються в Oracle: повне резервне копіювання, інкрементальне резервне копіювання, диференціальне резервне копіювання. Пояснення переваг і недоліків кожного типу.

3. Технологія Oracle Recovery Manager (RMAN). Розгляд основних можливостей та функцій RMAN для створення резервних копій і відновлення даних. Як RMAN автоматизує процес резервного копіювання та відновлення, а також управляє архівними журналами.

4. Налаштування та використання RMAN для резервного копіювання в Oracle. Кроки для налаштування RMAN, створення резервних копій за допомогою цього інструменту, налаштування архівних журналів для забезпечення безпеки даних.

5. Відновлення даних в Oracle. Опис процесу відновлення даних у СУБД Oracle, включаючи відновлення з повної резервної копії, інкрементальних та диференціальних копій. Розгляд процесу відновлення на рівні таблиць, баз даних або окремих файлів.

6. Стратегії відновлення після аварії в Oracle. Огляд стратегій відновлення бази даних після аварії. Як планувати аварійне відновлення, відновлення за допомогою резервних копій і архівних журналів, а також використання технології Flashback для відновлення даних.

7. Резервне копіювання та відновлення в середовищах Oracle Real Application Clusters (RAC). Особливості резервного копіювання та відновлення в кластерних середовищах Oracle RAC. Як забезпечується висока доступність даних і відновлення в кластерних середовищах.

8. Резервне копіювання та відновлення в хмарі з Oracle. Огляд процесів резервного копіювання та відновлення для баз даних Oracle в хмарних середовищах, зокрема в Oracle Cloud Infrastructure (OCI). Використання інструментів хмарного зберігання для збереження резервних копій.

9. Захист резервних копій даних в Oracle. Методи захисту резервних копій від несанкціонованого доступу. Використання шифрування для захисту резервних копій і гарантії їх цілісності.

10. Моніторинг та перевірка процесу резервного копіювання в Oracle. Огляд методів моніторингу та перевірки процесу резервного копіювання в Oracle. Як перевірити надійність резервних копій і виконання планів резервного копіювання за допомогою вбудованих інструментів Oracle.

Питання для самоперевірки з теми

1. Що таке резервне копіювання в СУБД Oracle, і чому цей процес є критичним для забезпечення безпеки даних?

2. Які основні типи резервних копій підтримуються в Oracle, і в чому полягає різниця між ними?

3. Як здійснюється створення повної резервної копії в Oracle? Які файли включає така копія?

4. Що таке інкрементальне резервне копіювання в Oracle, і як воно відрізняється від диференціального резервного копіювання?

5. Які переваги має використання Recovery Manager (RMAN) для резервного копіювання в Oracle?

6. Як налаштувати RMAN для створення резервних копій у Oracle? Які основні команди використовуються для цього?

7. Що таке архівні журнали в Oracle, і яку роль вони виконують у процесі резервного копіювання та відновлення даних?

8. Які параметри та налаштування необхідні для забезпечення успішного відновлення даних після аварії в Oracle?

9. Які основні стратегії відновлення після аварії підтримує Oracle? Як вони допомагають відновити дані до останнього відомого стану?

10. Як здійснюється відновлення бази даних з резервної копії в Oracle? Які основні кроки цього процесу?

11. Як здійснюється відновлення інкрементальних та диференціальних резервних копій в Oracle?

12. Які особливості резервного копіювання та відновлення в Oracle Real Application Clusters (RAC)?

13. Як здійснюється резервне копіювання і відновлення баз даних в хмарному середовищі Oracle Cloud?

14. Як забезпечується захист резервних копій даних в Oracle від несанкціонованого доступу? Які методи шифрування для цього використовуються?

15. Які методи моніторингу та перевірки процесу резервного копіювання в Oracle доступні для адміністраторів баз даних?

Тема 8. Робота з SQL.

1. Основи мови SQL в СУБД Oracle. Опис принципів роботи з SQL в СУБД Oracle. Основні SQL-команди та їх синтаксис для створення, модифікації та видалення даних в базах даних.

2. Створення та управління таблицями в Oracle. Огляд команд SQL для створення таблиць (CREATE TABLE), визначення типів даних, додавання та зміни стовпців (ALTER TABLE), видалення таблиць (DROP TABLE).

3. Основи маніпулювання даними в Oracle: SELECT, INSERT, UPDATE, DELETE. Розгляд основних SQL-команд для маніпулювання даними в Oracle: вибірка даних (SELECT), вставка нових рядків (INSERT), оновлення даних (UPDATE), видалення даних (DELETE).

4. Фільтрація та сортування даних в SQL. Огляд використання WHERE для фільтрації даних, а також команд для сортування результатів запитів (ORDER BY). Використання умов та операторів для точнішого пошуку даних.

5. Агрегатні функції та групування в SQL. Опис основних агрегатних функцій в SQL (COUNT, SUM, AVG, MIN, MAX) та їх застосування для групування даних (GROUP BY) і фільтрації груп (HAVING).

6.

7. Об'єднання таблиць за допомогою JOIN в SQL. Огляд різних типів JOIN (INNER JOIN, LEFT JOIN, RIGHT JOIN, FULL JOIN) для об'єднання даних з кількох таблиць. Синтаксис і приклади використання.

8. Підзапити в SQL. Розгляд концепції підзапитів: вкладені SELECT-запити для вибірки даних з іншої таблиці або результату іншого запиту.

9. Індекси та їх роль в покращенні продуктивності SQL-запитів в Oracle. Огляд індексів в СУБД Oracle: створення та управління індексами для прискорення пошуку та вибірки даних, а також типи індексів.

10. Транзакції в SQL: керування транзакціями та їх властивості (ACID). Опис транзакцій в SQL: початок, коміт та відкат транзакцій (COMMIT, ROLLBACK), а також їх властивості — атомарність, консистентність, ізоляція та довговічність (ACID).

11. Оптимізація SQL-запитів в Oracle. Розгляд методів оптимізації SQL-запитів для підвищення їх продуктивності: використання індексів, переписування запитів, аналіз виконання запитів (EXPLAIN PLAN).

12. Робота з великими обсягами даних в Oracle SQL. Огляд технік для обробки великих наборів даних: використання пагінації (LIMIT/OFFSET), оптимізація запитів для роботи з великими таблицями.

13. Робота з функціями та процедурами в Oracle SQL. Огляд створення та використання функцій і процедур у SQL для реалізації складних операцій та обробки даних на сервері.

14. Тимчасові таблиці та їх використання в SQL Oracle. Опис роботи з тимчасовими таблицями в Oracle для зберігання проміжних результатів при виконанні складних запитів або розрахунків.

Питання для самоперевірки з теми

1. Що таке SQL, і які основні команди використовуються для роботи з даними в СУБД Oracle?

2. Як створюється таблиця в Oracle за допомогою SQL? Які типи даних можна використовувати для стовпців таблиці?

3. Які команди SQL використовуються для додавання, оновлення та видалення даних в таблиці Oracle?

4. Як здійснюється вибірка даних з таблиці за допомогою команди SELECT? Які основні оператори для фільтрації використовуються?

5. Як використовуються оператори WHERE і HAVING для фільтрації даних в запитах SQL? У чому різниця між ними?

6. Що таке JOIN в SQL, і які типи об'єднання таблиць підтримуються в Oracle?

7. Як об'єднати таблиці за допомогою INNER JOIN, LEFT JOIN і RIGHT JOIN? Яка різниця між ними?

8. Що таке підзапит в SQL, і як його використовувати в Oracle для вибірки даних з іншої таблиці?

9. Що таке агрегатні функції в SQL? Які функції використовуються для підрахунку, обчислення суми, середнього значення, мінімуму та максимуму?

10. Як застосовувати GROUP BY для групування результатів SQL-запиту, і для чого використовуються агрегатні функції в поєднанні з цією командою?

11. Що таке ORDER BY, і як ним користуватися для сортування результатів запиту? Які параметри можна використовувати для сортування?

12. Як створювати індекси в Oracle, і для чого вони використовуються? Які типи індексів підтримує Oracle?

13. Що таке транзакція в SQL, і які операції виконуються в межах транзакції в Oracle?

14. Які команди використовуються для керування транзакціями в Oracle? Як відновити або скасувати транзакцію?

15. Що таке нормалізація бази даних? Як вона допомагає зберігати цілісність і ефективність даних у таблицях?

16. Як оптимізувати SQL-запити для поліпшення продуктивності в Oracle? Які інструменти та стратегії використовуються для цього?

17. Що таке тимчасові таблиці в Oracle, і як їх використовувати для зберігання проміжних результатів запитів?

18. Що таке функції та процедури в SQL? Як створити функцію або процедуру в Oracle?

Тема 9. Мова програмування PL/SQL.

1. Вступ до PL/SQL. Основи мови та її роль у СУБД Oracle. Огляд мови програмування PL/SQL, її призначення та застосування в СУБД Oracle. Різниця між SQL та PL/SQL, переваги використання PL/SQL для обробки даних на сервері.

2. Структура програм PL/SQL. Блоки коду. Опис структури програми в PL/SQL: оголошення змінних, обробка виключень, основні компоненти блоку (DECLARE, BEGIN, EXCEPTION, END). Як створюються програми та процеси у PL/SQL.

3. Змінні та типи даних у PL/SQL. Огляд змінних в PL/SQL: синтаксис оголошення змінних, типи даних, що підтримуються в PL/SQL. Використання скалярних типів, складених типів, табличних типів та типів об'єктів.

4. Умовні оператори та цикли в PL/SQL. Розгляд умовних операторів (IF...THEN, CASE) та циклів (LOOP, FOR, WHILE) для управління потоком виконання програми. Приклади використання умовних конструкцій для прийняття рішень.

5. Обробка виключень у PL/SQL. Огляд механізмів обробки помилок та виключень у PL/SQL: типи виключень (передвстановлені та визначені користувачем), блоки EXCEPTION, обробка помилок на різних рівнях програми.

6. Процедури та функції в PL/SQL. Опис створення та використання процедур та функцій у PL/SQL. Визначення параметрів, типів значень (вхідні, вихідні, вхідно-вихідні параметри). Різниця між функцією та процедурою.

7. Курсори в PL/SQL. Огляд курсорів у PL/SQL: явні та неявні курсори, робота з множиною рядків. Операції відкриття, закриття, отримання результатів з курсора.

8. Тригери в PL/SQL. Огляд тригерів у PL/SQL: типи тригерів (BEFORE, AFTER, INSTEAD OF), події, на які реагує тригер. Як використовувати тригери для автоматизації операцій в базі даних.

9. Об'єктно-орієнтовані можливості в PL/SQL. Розгляд об'єктно-орієнтованих можливостей у PL/SQL. Визначення об'єктів, класів, методів. Як створювати об'єкти в PL/SQL та працювати з ними.

10. Оптимізація програм у PL/SQL. Методи покращення продуктивності програм в PL/SQL. Використання масивів, мінімізація викликів курсорів, ефективне використання пам'яті. Огляд інструментів для профілювання та налагодження PL/SQL коду.

11. Динамічний SQL у PL/SQL. Використання динамічних запитів у програмах PL/SQL за допомогою команд EXECUTE IMMEDIATE та OPEN FOR. Як працювати з динамічними об'єктами бази даних.

12. Транзакції в PL/SQL. Як PL/SQL підтримує транзакції. Автоматичне керування транзакціями в межах програм. Використання COMMIT, ROLLBACK для завершення або скасування транзакцій.

Питання для самоперевірки з теми

1. Що таке PL/SQL і чим він відрізняється від звичайного SQL в Oracle?
2. Які основні компоненти блоку коду в PL/SQL? Опишіть структуру базового блоку.
3. Як оголосити змінні в PL/SQL? Які типи даних підтримує PL/SQL?
4. Що таке оператори умовного виконання в PL/SQL? Як використовуються оператори IF та CASE?
5. Як працюють цикли в PL/SQL? Наведіть приклади використання циклів LOOP, FOR та WHILE.

6. Що таке обробка виключень у PL/SQL? Як використовувати блок EXCEPTION для обробки помилок?

7. Як створюються та використовуються процедури в PL/SQL? Яка різниця між процедурами та функціями?

8. Що таке курсори в PL/SQL? Як використовуються явні та неявні курсори?

9. Як працює команда OPEN, FETCH, CLOSE з курсорами в PL/SQL? Як правильно використовувати ці команди?

10. Що таке тригери в PL/SQL? Як створюються тригери і для яких подій вони можуть бути використані?

11. Що таке динамічний SQL і як використовувати команду EXECUTE IMMEDIATE в PL/SQL?

12. Як працювати з типами даних у PL/SQL? Як оголошуються складені та об'єктні типи?

13. Як можна оптимізувати програми PL/SQL для підвищення продуктивності?

14. Що таке транзакції в PL/SQL? Як використовуються команди COMMIT та ROLLBACK для керування транзакціями?

Тема 10. Розробка програмних застосунків в Oracle APEX.

1. Вступ до Oracle APEX. Огляд платформи та її можливостей. Опис Oracle APEX (Application Express), її призначення та основних можливостей для швидкої розробки веб-застосунків на базі Oracle. Порівняння з іншими платформами для розробки веб-застосунків.

2. Створення та налаштування робочого середовища в Oracle APEX. Кроки для налаштування та використання Oracle APEX. Як налаштувати середовище для розробки застосунків, створення робочого простору та доступ до бази даних.

3. Основи розробки застосунків в Oracle APEX. Огляд основних компонентів Oracle APEX. Створення сторінок, зв'язок з базою даних, побудова інтерфейсу користувача за допомогою візуальних компонентів.

4. Робота з таблицями та даними в Oracle APEX. Створення таблиць, введення та редагування даних через форми та звіти, використання SQL-запитів у застосунках.

5. Створення форм і звітів в Oracle APEX. Як створювати інтерактивні форми та звіти в Oracle APEX для введення, редагування та виведення даних. Використання механізмів фільтрації та сортування.

6. Робота з динамічними діями в Oracle APEX. Огляд динамічних дій (Dynamic Actions). Створення подій та відповідних реакцій на події, взаємодія з елементами інтерфейсу користувача.

7. Безпека та доступ в Oracle APEX. Розгляд механізмів безпеки в Oracle APEX. Автентифікація, авторизація, створення ролей і керування доступом до застосунків і даних.

8. Інтеграція з іншими технологіями та сервісами. Як Oracle APEX може інтегруватися з іншими системами і сервісами, включаючи RESTful API, використання сторонніх бібліотек JavaScript та CSS для кастомізації.

9. Налаштування повідомлень та електронної пошти в Oracle APEX. Огляд можливостей для налаштування автоматичних повідомлень та відправки електронних листів з застосунків Oracle APEX, включаючи використання SQL та PL/SQL для генерації повідомлень.

10. Оптимізація продуктивності в Oracle APEX. Стратегії для оптимізації продуктивності застосунків, побудованих в Oracle APEX: використання індексів, кешування, зменшення затримок у запитах та відображеннях.

11. Розгортання застосунків в Oracle APEX. Опис процесу публікації та розгортання веб-застосунків, розроблених в Oracle APEX, на різних середовищах, включаючи локальне розгортання та хмарні платформи Oracle.

12. Моніторинг і підтримка застосунків в Oracle APEX. Огляд інструментів для моніторингу використання та продуктивності застосунків Oracle APEX, а також стратегій для їх підтримки та вдосконалення.

13. Підключення до зовнішніх джерел даних в Oracle APEX. Як налаштувати підключення до зовнішніх баз даних та API, обробляти дані з інших джерел у застосунках Oracle APEX.

14. Мобільні застосунки в Oracle APEX. Створення мобільних веб-застосунків за допомогою Oracle APEX. Адаптивний дизайн, інтеграція з мобільними пристроями, оптимізація інтерфейсу для мобільних користувачів.

15. Кращі практики розробки в Oracle APEX. Огляд кращих практик при розробці застосунків у Oracle APEX – проектування архітектури, створення адаптивного інтерфейсу, тести, документація та забезпечення якості.

Питання для самоперевірки з теми

1. Що таке Oracle APEX і які його основні можливості?
2. Як налаштувати робоче середовище для розробки в Oracle APEX?
3. Як створюється перший застосунок в Oracle APEX?
4. Які елементи містить структура програми в Oracle APEX?
5. Як створюються таблиці і форми для введення даних в Oracle APEX?
6. Як використовуються SQL-запити для роботи з даними в Oracle APEX?
7. Як створюються звіти в Oracle APEX і які типи звітів підтримуються?
8. Що таке динамічні дії в Oracle APEX і як вони використовуються?
9. Як налаштувати безпеку в Oracle APEX для обмеження доступу до застосунків?
10. Як працює автентифікація і авторизація користувачів в Oracle APEX?
11. Як налаштувати електронні повідомлення в Oracle APEX?

12. Як можна інтегрувати Oracle APEX із зовнішніми системами та сервісами?

13. Які методи використовуються для оптимізації продуктивності в Oracle APEX?

14. Як розгортати застосунки в Oracle APEX на сервері?

15. Як моніторити і підтримувати застосунки в Oracle APEX після їх розгортання?

3.3 Теми рефератів (доповідей)

1. Основи інформаційної безпеки в розподілених базах даних.
2. Захист конфіденційності даних у розподілених системах.
3. Визначення та запобігання загрозам для безпеки розподілених баз даних.
4. Методи шифрування даних у розподілених системах.
5. Аутентифікація та авторизація в розподілених базах даних.
6. Механізми контролю доступу в розподілених системах.
7. Архітектура захисту розподілених баз даних.
8. Технічні засоби захисту даних в розподілених базах даних.
9. Система безпеки Oracle Database.
10. Проблеми безпеки в хмарних базах даних.
11. Методи захисту даних у базах даних на основі блокчейн.
12. Керування доступом в СУБД Oracle.
13. Використання криптографії для захисту даних в СУБД Oracle.
14. Безпека та захист від SQL-ін'єкцій у СУБД Oracle.
15. Моніторинг безпеки в розподілених базах даних.
16. Резервне копіювання та відновлення даних у розподілених базах даних.
17. Використання Oracle Data Guard для забезпечення високої доступності.

18. Відновлення даних після аварій в Oracle Database.

19. Створення безпечних застосунків на основі бази даних Oracle.

20. Захист баз даних від несанкціонованого доступу.

21. Взаємодія між розподіленими базами даних і сторонніми системами.

22. Інтеграція та захист даних у гібридних хмарних середовищах.

23. Використання Oracle APEX для розробки безпечних веб-застосунків.

24. Основи проектування розподілених баз даних.

25. Перспективи розвитку технологій безпеки в розподілених базах даних.

26. Шифрування даних в транзиті в розподілених системах.

27. Використання багатообчислювальних середовищ для захисту даних.

28. Перевірка та аудит безпеки в розподілених базах даних.

29. Використання даних з API для безпечної роботи розподілених баз даних.

30. Підвищення надійності баз даних через механізми реплікації.

31. Проблеми та рішення в управлінні ідентифікацією користувачів у розподілених базах.

32. Використання PL/SQL для розробки безпечних програм в Oracle.

33. Методи аудиту та моніторингу для захисту даних в розподілених базах.

34. Використання Oracle Audit Vault для забезпечення безпеки даних.

35. Аномальна поведінка користувачів як загроза для безпеки даних.

36. Захист конфіденційності даних в базах даних для державних установ.

37. Методи тестування безпеки розподілених баз даних.

38. Проблеми безпеки при використанні великих даних в розподілених системах.

39. Стратегії відновлення даних в хмарних базах даних.

40. Використання технік шифрування для захисту великих обсягів даних.

41. Перспективи розвитку штучного інтелекту для захисту розподілених баз даних.

42. Вплив цифрових підписів на безпеку даних у базах даних.

43. Захист інформаційних систем у банківському секторі України.

44. Використання механізмів управління правами доступу в SSO для розподілених баз.

45. Аналіз сучасних загроз для баз даних у фінансовому секторі.

46. Технічні вимоги до захисту даних в сучасних розподілених системах.

47. Використання шифрування даних у реляційних базах даних.

48. Оцінка ефективності систем захисту даних у розподілених базах.

49. Техніки побудови архітектури для захисту даних у хмарних розподілених базах.

50. Вплив нормативних актів на захист інформації в українських базах даних.

4 ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ТА ВИМОГИ ДО РОБОТИ

4.1 Вимоги до виконання самостійної роботи

При виконанні самостійної роботи необхідно дотримуватись таких вимог:

– теоретичні питання та умови задач вибираються студентом згідно відповідного варіанту та наводяться перед відповіддю та відповідним рішенням;

– розв’язок задач має супроводжуватись поясненням, при необхідності, формулами тощо.

– самостійна робота повинна бути оформлена в електронному вигляді та надіслана у відповідні встановлені строки;

– сторінки роботи повинні бути пронумеровані, а також мати поля для зауважень;

– в кінці самостійної роботи наводиться список використаної студентом літератури згідно встановлених вимог.

При неповному та неправильному (виконано правильно менше 60% завдань) виконанні самостійної роботи, недотриманні умов вибору варіанту і порушенні інших вимог самостійна робота не зараховується.

4.2 Вимоги до змісту самостійної роботи

Пояснювальна записка реферату (доповіді) повинна містити наступні розділи:

– титульний лист (див. Додаток А);

– зміст;

– список використаної літератури.

4.3 Вимоги до оформлення самостійної роботи

Самостійна робота має бути набрана 14 кеглем, з полуторним інтервалом, на аркуші паперу формату А4, з полями таких розмірів:

– верхнє поле – 25 мм;

– нижнє поле: до тексту – 35 мм, до колонцифри – 25 мм;

– внутрішнє поле – 25 мм;

– зовнішнє поле – 25 мм.

Номери сторінок проставляють на нижньому полі аркуша посередині, починаючи з третьої, дотримуючись наскрізної нумерації без пропусків і буквених доповнень. Титульний аркуш включають до загальної нумерації сторінок. Номер сторінки на титульному аркуші не проставляють.

У текстовій частині:

– заголовки розміщуються посередині рядка та друкуються великими літерами без крапки в кінці, без підкреслення;

– заголовки підрозділів, пунктів і підпунктів тексту друкуються з великої літери (без підкреслення) без крапки в кінці;

– усі заголовки мають бути супідрядними і відповідати змісту роботи, абревіатури в заголовках не вживають, їх треба розшифровувати в тексті;

– заголовки з двох чи більше речень слід відокремлювати крапками;

– відстань між заголовком і текстом становить 28 пт, відстань між заголовками розділу та підрозділу – 14 пт;

– заголовок не розміщують внизу сторінки, якщо після нього уміщується лише один рядок тексту;

– таблиці та ілюстрації мають бути пронумерованими і міститися після посилань на них у тексті, примітки друкують під таблицею;

– у додатках розміщують офіційні, допоміжні і розрахункові матеріали, висновки, тощо, всі додатки нумеруються. Нумерація формул, таблиць і рисунків у кожному з додатків має бути самостійною.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Схемоконспект лекцій з навчальної дисципліни «Захист розподілених баз даних та інформаційних систем» : ел. навч.-наоч. посіб. для студентів всіх форм навчання галузі знань 12 Інформаційні технології / уклад. Я.Ю. Дорогий. – Луцьк : ДонНТУ, 2023. – 501 с. – Режим доступу: https://surl.li/daalny. – Назва з екрану.
2. Сагайда П.І. Розробка та організація баз даних у системах автоматизації проектування та управління: навч. посіб. для студентів спеціальності 7.080402. / П.І. Сагайда. – Краматорськ.: ДДМА, 2020. – 160 с.
3. Ярцев В.П. Організація баз даних та знань: навч. посіб. / В.П. Ярцев. – Київ : ДУТ 2018. – 214 с.
4. Ярцев В.П. Розподілені бази даних: навч. посіб. / В.П. Ярцев. – Київ : ДУТ 2018. – 97 с.
5. Глоба Л.С. Розробка інформаційних ресурсів та систем. Том 1: Розподілені системи [Електронний ресурс] / Л.С. Глоба. – Режим доступу: https://surl.li/xiocse. – Назва з екрана.
6. Глоба Л.С. Розробка інформаційних ресурсів та систем. Том 2: Розподілені системи [Електронний ресурс] / Л.С. Глоба. – Режим доступу: https://surl.gd/sjkbnp. – Назва з екрана.
7. Корнієнко С. К. Системи баз даних: організація та проектування: навч. посіб. / С. К. Корнієнко. – Запоріжжя : ЗНТУ, 2019. – 252 с.

ДОДАТОК А ПРИКЛАД ТИТУЛЬНОГО ЛИСТА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра прикладної математики та інформатики

РЕФЕРАТ (ДОПОВІДЬ)

з дисципліни «ЗАХИСТ РОЗПОДІЛЕНИХ БАЗ ДАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ»

Варіант №5

Виконав студент гр. ІПЗ-21

Водомір П.Ф.

Перевірив проф. каф. ПМІ

Дорогий Я.Ю.

Дрогобич, 2025

ДонНТУ

ПРИМІТКИ