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

15.03.2025

Захист інформації в розподілених системах

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 004.775.056.5:004.75](072)

З - 38

Захист інформації в розподілених системах. 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 : ДонНТУ, 2025. – 52 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 Сікорського

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 150 годин на дисципліну, 16 виділяється на практичні заняття та 102 – 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 інформації в розподілених системах» спрямована на забезпечення студентів необхідними знаннями та практичними навичками у галузі захисту інформації, що оброблюється 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 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:

ЗК10. Здатність зберігати та примножувати моральні, культурні, нвукові цінності 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.

ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп’ютерної інженерії.

ФК02. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

ФК03. Здатність створювати системне та прикладне програмне забезпечення комп’ютерних систем та мереж.

ФК04. Здатність забезпечувати захист інформації, що обробляється в комп’ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

ФК05. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

ФК06. Здатність проектувати, впроваджувати та обслуговувати комп’ютерні системи та мережі різного виду та призначення.

ФК07. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

ФК08. Готовність брати участь у роботах з впровадження комп’ютерних систем та мереж, введення їх до експлуатації на об’єктах різного призначення.

ФК09. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

ФК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

ФК11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

ФК12. Здатність ідентифікувати, класифікувати та описувати роботу програмно- технічних засобів, комп'ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.

ФК13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

ФК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

Програмні результати навчання за дисципліною наступні:

– ПРН 01. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

– ПРН 03. Знати новітні технології в галузі комп'ютерної інженерії.

– ПРН 04. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

– ПРН 05. Мати знання основ економіки та управління проектами.

– ПРН 06. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

– ПРН 08. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

– ПРН 09. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

– ПРН 11. Вміти здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії.

– ПРН 16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

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;

– принципи створення та підтримки захищених ІКС, побудованих на базі технологій Cisco.

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;

– проектувати та підтримувати захищені ІКС на базі технологій Cisco.

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 та мережного обладнання Cisco 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 IOS 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 захищених розподілених ІКС на базі технологій Cisco», «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», «Технології та обладнання для забезпечення захисту інформації в ІКС на базі технологій Cisco», «Захист інформації на кінцевих пристроях», «Технологія брандмауерів Cisco», «Технологія IPS Cisco», «Захист інформації в ОС Windows», «Захист інформації в ОС Linux», «Захист інформації в ОС Android», «Захист інформації в ОС MacOS».

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: одноріvнева, 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 захищених розподілених ІКС на базі технологій Cisco.

1. Вступ до архітектури захищених розподілених ІКС на базі технологій Cisco. Огляд платформи та її можливостей. Опис основних концепцій розподілених ІКС на базі технологій Cisco. Порівняння Cisco з іншими технологіями для побудови захищених розподілених мереж.

2. Створення та налаштування робочого середовища в Cisco. Кроки для налаштування мережевого середовища для побудови захищених ІКС. Як налаштувати основні компоненти мережі, включаючи маршрутизатори, комутатори та брандмауери Cisco.

3. Основи архітектури захищених ІКС на базі Cisco. Огляд основних компонентів архітектури захищених ІКС за допомогою Cisco: мережеві компоненти, безпека на рівні периметра, контроль доступу та аутентифікація користувачів.

4. Захист даних у розподілених ІКС за допомогою Cisco. Як забезпечити захист даних на периметрі і в середині мережі через використання технологій шифрування, VPN та інших методів захисту в рамках ІКС на базі Cisco.

5. Керування політиками безпеки в Cisco. Опис налаштування і застосування політик безпеки в Cisco для управління доступом до мережі та даних в розподілених ІКС.

6. Технічні аспекти побудови захищених розподілених ІКС з використанням Cisco. Огляд найкращих практик для проектування і реалізації захищених розподілених інформаційно-комунікаційних систем на базі Cisco, включаючи інтеграцію з іншими технологіями безпеки та масштабування системи.

Питання для самоперевірки з теми

1. Що таке архітектура захищених розподілених ІКС, і які основні концепції використовуються в технологіях Cisco для її побудови?

2. Які основні компоненти складають розподілену ІКС на базі технологій Cisco, і як вони взаємодіють для забезпечення безпеки мережі?

3. Як порівняти технології Cisco з іншими платформами для побудови захищених розподілених мереж? Які їх переваги та недоліки?

4. Як налаштувати мережеве середовище для побудови захищених ІКС за допомогою технологій Cisco? Які основні кроки для налаштування маршрутизаторів, комутаторів і брандмауерів?

5. Як забезпечити захист даних на периметрі і в середині мережі за допомогою технологій Cisco? Які методи шифрування та VPN використовуються для цього?

6. Як здійснюється контроль доступу в розподілених ІКС на базі Cisco, і які механізми аутентифікації користувачів застосовуються для забезпечення безпеки?

7. Які методи Cisco використовує для захисту даних в розподілених ІКС, зокрема для захисту від несанкціонованого доступу і витоків інформації?

8. Як налаштувати та застосувати політики безпеки в Cisco для управління доступом до мережі та даних в розподілених ІКС?

9. Які основні технічні аспекти необхідно враховувати при проектуванні захищених розподілених ІКС за допомогою Cisco?

10. Які кращі практики Cisco використовуються для інтеграції з іншими технологіями безпеки в розподілених ІКС і для масштабування системи?

Тема 4. 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 5. 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 6. 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 7. 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 8. 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 9. Технології та обладнання для забезпечення захисту інформації в ІКС на базі технологій Cisco.

1. Основи технологій захисту інформації в ІКС на базі Cisco. Огляд основних технологій Cisco для забезпечення безпеки в інформаційно-комунікаційних системах (ІКС), зокрема щодо захисту мережевих периметрів, даних та користувачів.

2. Огляд обладнання Cisco для забезпечення захисту ІКС. Опис основних моделей мережевого обладнання Cisco, таких як маршрутизатори, комутатори, брандмауери, що використовуються для захисту інформаційних систем.

3. Механізми шифрування даних в Cisco для захисту інформації. Огляд технологій шифрування, таких як IPsec і SSL, для забезпечення конфіденційності та захисту даних у розподілених ІКС на базі Cisco.

4. Використання Cisco forensics для аналізу та реагування на інциденти. Як Cisco використовує методи цифрової криміналістики для збору даних про інциденти безпеки, їх аналізу та реагування на загрози в розподілених ІКС.

5. Роль Cisco Identity Services Engine (ISE) в управлінні доступом. Огляд можливостей Cisco ISE для автентифікації та авторизації користувачів і пристроїв, а також для моніторингу та керування доступом у мережах ІКС.

6. Захист бездротових мереж в ІКС за допомогою технологій Cisco. Опис технологій захисту бездротових мереж, таких як Cisco Wireless LAN Controller та Cisco Umbrella, для забезпечення безпеки в ІКС.

7. Масштабування та управління безпекою в ІКС на базі Cisco. Як масштабувати мережеву інфраструктуру Cisco для підтримки великих і складних інформаційних систем, зокрема в умовах високої доступності та резервування.

Питання для самоперевірки з теми

1. Які основні технології Cisco використовуються для забезпечення безпеки в інформаційно-комунікаційних системах (ІКС)?

2. Як Cisco забезпечує захист мережевих периметрів, даних та користувачів у розподілених ІКС?

3. Які основні моделі мережевого обладнання Cisco застосовуються для захисту інформаційних систем, і які функції вони виконують?

4. Як технології шифрування, такі як IPsec та SSL, використовуються Cisco для забезпечення конфіденційності та захисту даних у розподілених ІКС?

5. Що таке Cisco forensics, і як вона застосовується для збору та аналізу даних при інцидентах безпеки?

6. Як Cisco Identity Services Engine (ISE) допомагає в управлінні доступом в ІКС?

7. Які механізми автентифікації та авторизації використовуються Cisco ISE для забезпечення безпеки доступу до мереж?

8. Як Cisco захищає бездротові мережі в ІКС за допомогою технологій, таких як Cisco Wireless LAN Controller та Cisco Umbrella?

9. Як масштабується мережеве середовище Cisco для підтримки великих і складних інформаційних систем з високими вимогами до безпеки?

10. Які стратегії Cisco застосовує для забезпечення високої доступності та резервування в розподілених ІКС?

Тема 10. Захист інформації на кінцевих пристроях.

1. Основи захисту інформації на кінцевих пристроях. Опис основних концепцій і принципів захисту інформації на кінцевих пристроях, таких як комп'ютери, смартфони, планшети та інші гаджети. Розгляд типових загроз і вразливостей для кінцевих пристроїв.

2. Захист кінцевих пристроїв від шкідливих програм. Огляд методів захисту від шкідливих програм, таких як віруси, трояни, шпигунські програми. Використання антивірусних програм і фаєрволів для забезпечення безпеки пристроїв.

3. Шифрування даних на кінцевих пристроях. Як здійснюється шифрування даних на кінцевих пристроях для захисту інформації в разі втрати або крадіжки пристрою. Огляд технологій шифрування, таких як BitLocker, FileVault, VeraCrypt.

4. Методи аутентифікації на кінцевих пристроях. Розгляд різних методів аутентифікації користувачів на кінцевих пристроях: паролі, біометрія, багатофакторна автентифікація.

5. Політики безпеки для кінцевих пристроїв. Опис політик безпеки для управління доступом, захисту даних та конфіденційності на кінцевих пристроях у корпоративних середовищах. Як налаштувати політики безпеки для мобільних пристроїв і ПК.

6. Захист мобільних пристроїв. Специфіка захисту мобільних пристроїв від атак і вразливостей. Використання мобільних антивірусів, VPN, шифрування даних, та політики управління мобільними пристроями (MDM).

7. Ризики при використанні зовнішніх носіїв даних на кінцевих пристроях. Огляд загроз, пов'язаних з використанням USB-носіїв, зовнішніх

жорстких дисків та інших зовнішніх пристроїв для зберігання даних. Методи захисту даних на таких носіях.

8. Безпека при використанні хмарних сервісів на кінцевих пристроях. Ризики та методи захисту при зберіганні даних на хмарних сервісах за допомогою кінцевих пристроїв. Використання шифрування і політик доступу до хмарних даних.

9. Мережеві атаки на кінцеві пристрої та їх захист. Опис типових мережевих атак на кінцеві пристрої, таких як Man-in-the-Middle, фішинг та атак на Wi-Fi з'єднання. Методи захисту від таких атак.

10. Оновлення програмного забезпечення на кінцевих пристроях. Важливість регулярних оновлень програмного забезпечення та безпеки на кінцевих пристроях. Як налаштувати автоматичне оновлення та забезпечити своєчасне виправлення вразливостей.

Питання для самоперевірки з теми

1. Які основні концепції та принципи захисту інформації на кінцевих пристроях, таких як комп'ютери, смартфони та планшети?

2. Які типові загрози та вразливості існують для кінцевих пристроїв і як вони можуть впливати на безпеку?

3. Які методи захисту кінцевих пристроїв від шкідливих програм є найбільш ефективними, і як працюють антивірусні програми та фаєрволи?

4. Як здійснюється шифрування даних на кінцевих пристроях і які технології шифрування існують для захисту інформації у разі втрати пристрою?

5. Які методи аутентифікації використовуються на кінцевих пристроях для забезпечення доступу до даних?

6. Як налаштувати політики безпеки для мобільних пристроїв і ПК в корпоративних середовищах, щоб забезпечити захист інформації?

7. Які специфічні ризики існують при використанні мобільних пристроїв і як їх можна захистити від атак і вразливостей?

8. Які загрози пов'язані з використанням зовнішніх носіїв даних на кінцевих пристроях і як можна захистити дані на таких носіях?

9. Як можна забезпечити безпеку при зберіганні даних на хмарних сервісах за допомогою кінцевих пристроїв?

10. Чому важливо регулярно оновлювати програмне забезпечення на кінцевих пристроях і які кроки потрібно зробити для забезпечення автоматичного оновлення та виправлення вразливостей?

Тема 11. Технологія брандмауерів Cisco.

1. Основи технології брандмауерів Cisco. Огляд технологій брандмауерів Cisco, їх призначення та роль у захисті мереж від несанкціонованого доступу. Порівняння різних типів брандмауерів та їх функцій у рамках інфраструктури Cisco.

2. Типи брандмауерів Cisco та їх особливості. Опис основних типів брандмауерів Cisco: фаєрволи нового покоління (NGFW), Stateful Inspection, Application Layer Filtering. Різниця між програмними і апаратними брандмауерами.

3. Створення та налаштування брандмауерів Cisco. Кроки для налаштування брандмауера Cisco: конфігурація правил доступу, визначення політик безпеки, управління трафіком і моніторинг подій. Огляд процесу налаштування базових і просунутих функцій брандмауерів Cisco.

4. Інтеграція брандмауерів Cisco в мережеву інфраструктуру. Як брандмауери Cisco інтегруються з іншими мережевими пристроями, такими як маршрутизатори, комутатори та системи виявлення і запобігання вторгненням (IDS/IPS).

5. Контроль доступу за допомогою брандмауерів Cisco. Фільтрація трафіку, моніторинг з’єднань та обмеження доступу за IP-адресами, портами та протоколами.

6. Механізми шифрування та VPN у брандмауерах Cisco. Огляд методів шифрування і налаштування VPN (Virtual Private Network) для захищеного

з’єднання через брандмауери Cisco, включаючи використання IPsec, SSL і DMVPN.

7. Захист мережевих периметрів за допомогою брандмауерів Cisco. Як Конфігурація фільтрації трафіку, захист від DDoS-атак, моніторинг вхідних і вихідних з’єднань.

8. Моделі брандмауерів Cisco та їх роль у корпоративних мережах. Огляд моделей брандмауерів Cisco, таких як Cisco ASA (Adaptive Security Appliance), Firepower, та їх використання в корпоративних мережах для забезпечення безпеки.

9. Моніторинг і аналіз роботи брандмауерів Cisco. Аналіз журналів подій, налаштування алертів і трекінг продуктивності брандмауерів у мережі.

10. Інтеграція брандмауерів Cisco з системами управління безпекою. Взаємодія брандмауерів Cisco з іншими системами безпеки, такими як SIEM (Security Information and Event Management), для більш ефективного управління загрозами та реагування на інциденти.

Питання для самоперевірки з теми

1. Які основні функції виконують брандмауери Cisco у захисті мережі?
2. Які типи брандмауерів Cisco існують і чим вони відрізняються один від одного?
3. Як налаштувати базову конфігурацію брандмауера Cisco для фільтрації трафіку?
4. Що таке Stateful Inspection в брандмауерах Cisco і як він працює?
5. Як брандмауери Cisco інтегруються з іншими мережевими пристроями, такими як маршрутизатори та комутатори?
6. Які механізми шифрування використовуються у брандмауерах Cisco для забезпечення безпеки трафіку?
7. Як налаштувати Virtual Private Network (VPN) на брандмауері Cisco для забезпечення захищеного з'єднання?

8. Які методи брандмауери Cisco використовують для захисту мережевого периметра від зовнішніх атак?

9. Як здійснюється моніторинг та аналіз роботи брандмауера Cisco, і як реагувати на загрози?

10. Як брандмауери Cisco допомагають у керуванні доступом до корпоративних ресурсів на основі правил безпеки?

Тема 12. Технологія IPS Cisco.

1. Основи технології IPS Cisco. Огляд основних технологій Cisco для виявлення та запобігання вторгненням.

2. Типи атак, що виявляються IPS Cisco. Опис основних атак, таких як DoS/DDoS, SQL ін'єкції та атак на прикладні рівні.

3. Архітектура і компоненти системи IPS Cisco. Опис архітектури IPS Cisco та основних компонентів системи.

4. Процес налаштування і конфігурації IPS Cisco. Кроки для налаштування IPS Cisco для захисту мережі.

5. Методи виявлення загроз в IPS Cisco. Використання підписів, поведінкового аналізу та аналізу аномалій для виявлення загроз.

6. Аналіз і реагування на інциденти за допомогою IPS Cisco. Як IPS Cisco реагує на загрози і нейтралізує їх у реальному часі.

7. Інтеграція IPS Cisco з іншими засобами безпеки. Способи інтеграції IPS Cisco з брандмауерами, SIEM та іншими системами.

8. Оновлення підписів і баз даних у IPS Cisco. Процес оновлення підписів та баз даних для підтримки актуальності захисту.

9. Роль IPS Cisco в побудові захищених мереж. Як IPS Cisco інтегрується в архітектуру захищених мереж.

10. Оцінка ефективності IPS Cisco та покращення захисту мережі. Методи оцінки ефективності IPS Cisco і вдосконалення політик безпеки.

Питання для самоперевірки з теми

1. Що таке технологія IPS Cisco і яку роль вона відіграє у забезпеченні безпеки мережі?
2. Які основні типи атак можуть бути виявлені за допомогою IPS Cisco?
3. Як працює архітектура системи IPS Cisco і які її основні компоненти?
4. Які кроки необхідно виконати для налаштування та конфігурації IPS Cisco в мережі?
5. Як IPS Cisco виявляє загрози за допомогою підписів, поведінкового аналізу та аналізу аномалій?
6. Які методи реагування на інциденти використовує IPS Cisco для нейтралізації загроз?
7. Як відбувається інтеграція IPS Cisco з іншими засобами безпеки, такими як брандмауери або системи моніторингу?
8. Як IPS Cisco підтримує актуальність своєї бази підписів і баз даних загроз?
9. Яку роль відіграє IPS Cisco в побудові захищених мереж і мережевих периметрів?
10. Як можна оцінити ефективність роботи IPS Cisco та вдосконалити політики безпеки в мережі?

Тема 13. Захист інформації в ОС Windows.

1. Основи захисту інформації в ОС Windows. Огляд основних принципів і технологій захисту інформації в операційних системах Windows. Роль Windows у захисті даних та управлінні доступом.
2. Політики безпеки в ОС Windows. Як налаштовуються політики безпеки в Windows, включаючи політики груп, локальні політики та політики для керування доступом до системи.
3. Автентифікація та авторизація в ОС Windows. Опис методів автентифікації та авторизації користувачів в Windows, включаючи паролі,

біометричні дані, ідентифікацію через смарт-карти та багатофакторну автентифікацію.

4. Захист від шкідливих програм в ОС Windows. Технології та інструменти для захисту від вірусів, троянських програм, шпигунських програм та інших загроз у Windows.

5. Використання вбудованих засобів захисту в ОС Windows. Огляд вбудованих інструментів Windows, таких як Windows Defender, брандмауер Windows, і BitLocker для захисту від загроз.

6. Шифрування даних в ОС Windows. Технології шифрування даних в Windows, включаючи використання BitLocker для шифрування дисків і EFS для шифрування файлів та папок.

7. Захист від атак через мережу в ОС Windows. Механізми захисту від мережевих атак, таких як фаєрволи, виявлення вторгнень і налаштування безпеки мережевих з'єднань у Windows.

8. Управління оновленнями безпеки в ОС Windows. Як здійснюється управління оновленнями безпеки, важливість регулярних оновлень та патчів для забезпечення безпеки системи.

9. Моніторинг безпеки в ОС Windows. Інструменти для моніторингу безпеки в Windows, включаючи журнали подій, System Center, та інші засоби для відслідковування діяльності системи.

10. Захист конфіденційності в ОС Windows. Методи захисту конфіденційності користувачів, зберігання паролів, керування правами доступу та захист персональних даних в Windows.

Питання для самоперевірки з теми

1. Які основні принципи захисту інформації реалізуються в ОС Windows?

2. Як налаштовуються політики безпеки в ОС Windows? Які основні типи політик існують?

3. Як працює автентифікація та авторизація користувачів в ОС Windows?

4. Які методи автентифікації доступні в ОС Windows, і як налаштувати багатофакторну автентифікацію?

5. Як працює Windows Defender і які функції він виконує для захисту комп'ютера?

6. Як налаштувати брандмауер Windows для блокування несанкціонованого доступу?

7. Як здійснюється шифрування даних у Windows за допомогою BitLocker? Які переваги та недоліки цього методу?

8. Як працює система шифрування EFS (Encrypting File System) у Windows і як налаштувати її для захисту файлів?

9. Які основні загрози для ОС Windows можуть виникнути через шкідливі програми, і як з ними боротися?

10. Як налаштувати безпеку мережевих з'єднань у Windows для захисту від атак через Інтернет?

11. Як здійснюється управління оновленнями безпеки в Windows? Яке значення має регулярне оновлення системи?

12. Як здійснюється моніторинг безпеки в ОС Windows за допомогою журналів подій?

13. Як налаштувати контролі доступу до системних ресурсів і файлів в ОС Windows?

14. Як можна захистити конфіденційність персональних даних на комп'ютері під управлінням Windows?

15. Як налаштувати і використовувати засоби для виявлення вторгнень і атак на комп'ютері з ОС Windows?

Тема 14. Захист інформації в ОС Linux.

1. Основи захисту інформації в ОС Linux. Огляд основних принципів та методів забезпечення безпеки в операційній системі Linux. Як Linux забезпечує захист даних і користувачів.

2. Керування доступом в ОС Linux. Опис механізмів контролю доступу в Linux, таких як користувацькі та групові права, ACL (Access Control Lists) та інші методи обмеження доступу до файлів і ресурсів.

3. Шифрування даних в ОС Linux. Огляд технологій шифрування, таких як LUKS (Linux Unified Key Setup), для захисту даних на дисках і пристроях, а також використання GPG для шифрування повідомлень та файлів.

4. Автентифікація та авторизація в ОС Linux. Як здійснюється автентифікація користувачів в Linux, використання паролів, SSH-ключів та інших методів доступу, таких як PAM (Pluggable Authentication Modules).

5. Захист від шкідливих програм в ОС Linux. Огляд методів захисту від шкідливих програм, таких як віруси, троянські програми, шпигунські програми, а також використання антивірусних програм для Linux.

6. Захист мережі в ОС Linux. Налаштування брандмауера в Linux за допомогою iptables або firewalld для захисту від несанкціонованого доступу до системи та мережі. Використання VPN для забезпечення безпеки мережевого трафіку.

7. Безпека при використанні користувацьких та системних облікових записів в Linux. Опис методів захисту облікових записів користувачів та адміністраторів, налаштування політик паролів, двофакторної автентифікації.

8. Моніторинг і аудит безпеки в ОС Linux. Використання журналів подій (syslog) та інструментів для моніторингу безпеки, таких як Auditd, для відслідковування змін в системі та виявлення можливих загроз.

9. Інструменти для захисту та виявлення вторгнень в ОС Linux. Огляд інструментів, таких як Fail2ban, AppArmor, SELinux для захисту системи від атак, виявлення вторгнень і захисту на рівні додатків.

10. Оновлення та управління патчами в ОС Linux. Як налаштувати автоматичне оновлення системи та програмного забезпечення в Linux для забезпечення актуальності патчів безпеки.

Питання для самоперевірки з теми

1. Які основні принципи забезпечення безпеки в операційній системі Linux?

2. Як працює контроль доступу в Linux, і як налаштовуються користувацькі та групові права доступу?

3. Що таке ACL (Access Control List), і як його використовувати для налаштування доступу в Linux?

4. Як здійснюється шифрування даних на диску за допомогою LUKS в Linux?

5. Як шифрувати файли і повідомлення в Linux, використовуючи GPG?

6. Які методи автентифікації користувачів підтримує ОС Linux, і чим відрізняються SSH-ключі від паролів?

7. Що таке PAM (Pluggable Authentication Modules), і як він допомагає в процесі автентифікації в Linux?

8. Які інструменти можна використовувати для захисту Linux від шкідливих програм, таких як віруси і троянські програми?

9. Як налаштувати брандмауер в Linux за допомогою iptables або firewalld?

10. Як забезпечити захист мережевого трафіку в Linux за допомогою VPN?

11. Як налаштовуються політики паролів для користувачів в Linux, і як забезпечується їхня безпека?

12. Які інструменти можна використовувати для моніторингу безпеки в Linux, і як вони допомагають виявляти загрози?

13. Як працює SELinux (Security-Enhanced Linux), і як він покращує безпеку Linux?

14. Як працює Fail2ban, і як цей інструмент допомагає захистити Linux від атак на паролі?

15. Як можна забезпечити актуальність патчів безпеки в Linux, і чому це важливо для захисту системи?

Тема 15. Захист інформації в ОС Android.

1. Основи захисту інформації в ОС Android. Огляд основних принципів і технологій забезпечення безпеки в операційній системі Android. Роль Android у захисті даних користувачів та додатків.

2. Методи автентифікації та авторизації в ОС Android. Опис методів автентифікації користувачів в Android, включаючи паролі, біометрію, розпізнавання обличчя та відбитків пальців, а також багатофакторну автентифікацію.

3. Захист даних на пристроях Android за допомогою шифрування. Як здійснюється шифрування даних на пристроях Android для захисту інформації в разі втрати або крадіжки пристрою. Огляд технологій шифрування, таких як шифрування всього диска (Full Disk Encryption, FDE) і шифрування файлів.

4. Управління доступом до додатків в ОС Android. Огляд механізмів управління доступом до додатків в Android, таких як права доступу до даних, дозволи на використання камери, мікрофона та інших пристроїв.

5. Захист від шкідливих програм в ОС Android. Методи захисту пристроїв Android від шкідливих програм, таких як віруси, трояни та шпигунські програми. Використання антивірусних програм і безпечних магазинів додатків.

6. Політики безпеки та контроль за оновленнями в Android. Огляд політик безпеки, які можна налаштувати в Android, а також важливість регулярних оновлень для підтримки безпеки системи та додатків.

7. Мобільний брандмауер для Android. Як налаштувати мобільний брандмауер на пристрої Android для захисту від небажаних з'єднань та атак.

8. Використання віртуальних приватних мереж (VPN) на пристроях Android. Як використовувати VPN для захисту даних при підключенні до незахищених мереж, таких як публічні Wi-Fi.

9. Ризики при використанні сторонніх додатків в ОС Android. Огляд ризиків, пов'язаних з використанням додатків із сторонніх джерел (поза Google Play), і як захистити пристрій від потенційних загроз.

10. Інструменти для моніторингу безпеки в ОС Android. Огляд інструментів для моніторингу безпеки на пристроях Android, таких як аналіз журналів подій, виявлення вторгнень і оцінка ризиків.

Питання для самоперевірки з теми

1. Які основні принципи захисту інформації реалізуються в ОС Android?
2. Як налаштовується автентифікація користувачів на пристроях Android, і які методи автентифікації доступні?
3. Як здійснюється шифрування даних на пристрої Android, і які технології шифрування використовуються для цього?
4. Як працює механізм управління доступом до додатків в Android, і що таке дозволи на доступ?
5. Які методи захисту від шкідливих програм існують для пристроїв Android?
6. Як налаштовуються політики безпеки в ОС Android для забезпечення захисту пристрою та додатків?
7. Як Android використовує брандмауери для захисту пристроїв, і які функції вони виконують?
8. Які основні ризики виникають при використанні додатків із сторонніх джерел на Android, і як можна захистити пристрій від цих загроз?
9. Як використовувати VPN на пристрої Android для забезпечення безпеки при підключенні до незахищених мереж Wi-Fi?
10. Які інструменти для моніторингу безпеки можна використовувати на пристроях Android для виявлення загроз і аналізу системи?

Тема 16. Захист інформації в ОС MacOS.

1. Основи захисту інформації в ОС MacOS. Огляд основних принципів і методів забезпечення безпеки в операційній системі MacOS. Роль MacOS у захисті даних і користувачів.

2. Автентифікація та авторизація в ОС MacOS. Опис методів автентифікації в MacOS, таких як паролі, біометрія (Touch ID, Face ID), і багатофакторна автентифікація.

3. Шифрування даних в ОС MacOS. Як здійснюється шифрування даних у MacOS за допомогою FileVault для захисту інформації у разі втрати або крадіжки пристрою.

4. Безпека при використанні додатків в ОС MacOS. Як MacOS забезпечує безпеку додатків через систему контрольованих дозволів і захист від шкідливих програм (Gatekeeper, XProtect).

5. Захист від шкідливих програм в ОС MacOS. Методи захисту MacOS від шкідливих програм, таких як віруси, трояни, шпигунські програми, за допомогою вбудованих інструментів і антивірусних програм.

6. Мережевий захист в ОС MacOS. Огляд механізмів захисту мережевих з'єднань, налаштування брандмауера, VPN і використання шифрування для захисту даних у мережах.

7. Політики безпеки та контроль доступу в ОС MacOS. Як налаштовуються політики безпеки та контроль доступу до системи і файлів через користувачів, групи та правила.

8. Моніторинг безпеки в ОС MacOS. Огляд інструментів для моніторингу безпеки в MacOS, таких як консоль журналів, системний монітор і сторонні програми для виявлення загроз.

9. Використання резервних копій і відновлення даних в ОС MacOS. Як використовувати Time Machine для створення резервних копій та відновлення даних на MacOS, забезпечення цілісності та доступності даних.

10. Захист конфіденційності в ОС MacOS. Методи забезпечення конфіденційності персональних даних у MacOS, включаючи налаштування прав доступу, використання шифрування і налаштування конфіденційності для додатків.

Питання для самоперевірки з теми

1. Які основні принципи забезпечення безпеки в операційній системі MacOS?
2. Як працює система автентифікації в MacOS, і які методи автентифікації доступні для користувачів?
3. Як шифрується диск на MacOS за допомогою FileVault і які переваги цього методу?
4. Які механізми захисту MacOS використовуються для запобігання установці шкідливих програм через додатки?
5. Як налаштувати брандмауер в MacOS для захисту від несанкціонованого доступу до системи?
6. Як MacOS забезпечує захист даних в мережевих з'єднаннях, і які інструменти підтримуються для підключення до VPN?
7. Як налаштувати політики безпеки в MacOS для управління доступом до файлів і системних ресурсів?
8. Які інструменти MacOS використовуються для моніторингу безпеки системи та виявлення потенційних загроз?
9. Як налаштувати Time Machine для створення резервних копій на MacOS і для забезпечення відновлення даних?
10. Які методи забезпечення конфіденційності персональних даних доступні в MacOS, і як їх налаштувати для захисту особистої інформації?

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. Захист баз даних від несанкціонованого доступу.

20. Взаємодія між розподіленими базами даних і сторонніми системами.

21. Інтеграція та захист даних у гібридних хмарних середовищах.

22. Основи проектування розподілених баз даних.

23. Перспективи розвитку технологій безпеки в розподілених базах даних.

24. Шифрування даних в транзиті в розподілених системах.

25. Використання багатообчислювальних середовищ для захисту даних.

26. Перевірка та аудит безпеки в розподілених базах даних.

27. Підвищення надійності баз даних через механізми реплікації.

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

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

30. Використання Oracle Audit Vault для забезпечення безпеки даних.

31. Аномальна поведінка користувачів як загроза для безпеки даних.

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

33. Методи тестування безпеки розподілених баз даних.

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

35. Стратегії відновлення даних в хмарних базах даних.

36. Використання технік шифрування для захисту великих обсягів даних.

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

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

39. Захист інформаційних систем у банківському секторі України.

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

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

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

43. Використання шифрування даних у реляційних базах даних.

44. Оцінка ефективності систем захисту даних у розподілених базах.

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

46. Впровадження брандмауерів Cisco в захисті корпоративних мереж.

47. Оцінка ефективності технології IPS Cisco в сучасних кіберзагрозах.

48. Захист інформації в ОС Windows: порівняння з іншими операційними системами.

49. Основи захисту кінцевих пристроїв в ОС Windows: від шкідливих програм до управління доступом.

50. Використання технології IPS Cisco для побудови захищених розподілених ІКС.

51. Захист інформації в ОС MacOS: підходи до захисту даних та персональної конфіденційності.

52. Технології шифрування даних в ОС Windows: ефективність і загрози.

53. Впровадження технологій IPS Cisco для захисту мереж в умовах високої доступності.

54. Шифрування даних на мобільних пристроях Android: технології та загрози.

55. Як забезпечити захист інформації в корпоративних мережах за допомогою брандмауерів Cisco?

56. Системи моніторингу загроз в мережах за допомогою Cisco Security Intelligence.

57. Оцінка безпеки кінцевих пристроїв: методи захисту інформації на комп'ютерах і мобільних пристроях.

58. Ризики при використанні зовнішніх носіїв для зберігання даних у системах Windows.

59. Методи та інструменти для контролю безпеки на кінцевих пристроях в ОС MacOS.

60. Захист мережі від DDoS-атак за допомогою технологій Cisco.

61. Захист даних у хмарі з використанням технологій шифрування в ОС Windows.

62. Шифрування та безпека даних у розподілених базах даних на платформі Cisco.

63. Методи автентифікації і авторизації користувачів в системах на базі технологій Cisco.

64. Проблеми та рішення щодо захисту інформації в хмарних технологіях за допомогою Cisco.

65. Стратегії захисту від SQL ін'єкцій та інших мережевих атак в системах на базі Cisco.

66. Методи оптимізації брандмауерів Cisco для великих підприємств.

67. Оцінка ефективності технології IPS Cisco в побудові захищених IT-інфраструктур.

68. Використання криптографії для забезпечення безпеки мобільних пристроїв в Android.

69. Механізми захисту та виявлення вторгнень в системах на базі ОС Linux.

70. Впровадження політик безпеки для операційних систем Android та IOS.

71. Забезпечення безпеки персональних даних за допомогою антивірусних програм в ОС Windows.

72. Оцінка впливу систем шифрування на ефективність роботи пристроїв MacOS.

73. Кращі практики управління ризиками та виявлення загроз в мобільних пристроях на базі Android.

74. Використання технологій Cisco для створення захищених VPN підключень в корпоративних мережах.

75. Шифрування в хмарних середовищах і захист конфіденційності в хмарних сервісах на базі Cisco.

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 інформації в розподілених системах» : ел. навч.-наоч. посіб. для студентів всіх форм навчання галузі знань 12 Інформаційні технології / уклад. Я.Ю. Дорогий. – Луцьк : ДонНТУ, 2024. – 1179 с. – Режим доступу: https://surl.li/cosbrx. – 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. – К. ДУТ 2018. – 97с.

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 екрану.

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 екрану.

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 ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ СИСТЕМАХ»

Варіант №7

Виконав студент гр. КІ-21

Солоденький В.А.

Перевірив проф. каф. ПМІ

Дорогий Я.Ю.

Дрогобич, 2025

ДонНТУ

ПРИМІТКИ