матричних диференціальних рівнянь. Для матричного диференціального рівняння Ляпунова перенесено методику побудови функції Ляпунова на основі матричного рівняння Ляпунова.

В третій частині обґрунтовано умови керованості лінійної дискретної системи зі зміною розмірності вектора стану за наявності обмежень на початковий і кінцевий стан, а також на функцію керування. У випадку відсутності обмежень на функцію керування запропоновано умови керованості і функцію керування, яка розв'язує задачу про переведення системи в окіл заданого фінального стану з мінімізацією норми функції керування [4].

В четвертій частині доповіді на основі критеріїв керованості пропонується методика створення інформаційної системи на виробничому підприємстві з функціонально стійким технологічним процесом [4,5]. Далі проаналізовано математичні моделі динаміки освітнього процесу і запропоновано критерії ефективності освітнього процесу на основі критеріїв керованості.

Список використаних джерел:

1. Башняков О.М., Гаращенко Ф.Г., Пічкур В.В. Практична стійкість, оцінки та оптимізація. – К.: Київський університет. - 2008. – 383 с.
2. Пічкур В.В., Мазур Д.А., Собчук В.В. Керованість лінійної дискретної системи зі зміною розмірності вектора стану. // Журнал обчислювальної та прикладної математики 2021, No 1 (135). 173 – 178
3. Капустян О.В., Пічкур В.В., Собчук В.В. Теорія динамічних систем. –Луцьк: Вежа-Друк, 2020.- -348 с.
4. PICHKUR, V.V. and SOBCHUK, V.V., 2021. Mathematical model and control design of a functionally stable technological process. Journal of Optimization, Differential Equations and their Applications, 29(1), pp. 32-41.
5. V. Sobchuk, V. Pichkur, O. Barabash, O. Laptiev, I. Kovalchuk and A. Zidan, Algorithm of Control of Functionally Stable Manufacturing Processes of Enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 206-210.

ПРОЗОРЕ ШИФРУВАННЯ В БАЗІ ДАНИХ ORACLE

Плоднік К. Ю., Булатецька Л. В.
Волинський національний університет імені Лесі Українки

Прозоре шифрування даних (Transparent Data Encryption (TDE) дозволяє шифрувати конфіденційні дані, що містяться в таблицях і табличних областях. Коли користувачі вводять дані, база даних прозоро шифрує ці дані і зберігає. Точно так же, коли користувачі вибирають ці дані, сервер баз даних автоматично розшифровує їх. Для попередження несанкціонованої розшифровки, TDE зберігає ключі шифрування в зовнішньому модулі безпеки по відношенню до бази даних. Користувач може шифрувати конфіденційні дані на рівні стовпців або табличного простору. Для шифрування стовпців і шифрування табличного

простору TDE використовує дворівневу архітектуру на основі ключів. Головний ключ шифрування доступний лише користувачеві, якому надано відповідні привілеї. Неавторизовані користувачі, такі як зловмисники, які намагаються здійснити атаки, не можуть прочитати дані зі сховища та резервного копіювання, якщо вони не мають головного ключа шифрування TDE для їх розшифрування. Для цього зовнішнього модуля безпеки Oracle Database використовує програмне сховище ключів Oracle (гаманець) або сховище ключів апаратного модуля безпеки (HSM). Зберігаючи таким чином головний ключа шифрування, TDE запобігає його несанкціонованому використанню. Використання зовнішнього модуля безпеки відокремлює звичайні функції програми від операцій шифрування, що дає змогу призначати окремі, чіткі обов'язки адміністраторам баз даних та адміністраторам безпеки. Безпека посилюється, оскільки пароль сховища ключів може бути невідомим адміністратору бази даних, що вимагає від адміністратора безпеки надати пароль.

На рівні стовпців користувач може шифрувати дані за допомогою вибраних стовпців таблиці. Якщо таблиця містить зашифровані стовпці, TDE використовує один ключ таблиці TDE незалежно від кількості зашифрованих стовпців. Кожен ключ окремо шифрується головним ключем. Усі ключі таблиці TDE розташовані разом у стовпці colklc таблиці словника даних ENC$. Жодні ключі не зберігаються у відкритому доступі.

Шифрування табличного простору прозорого шифрування даних (TDE) дає змогу зашифрувати весь табличний простір. Усі об'єкти, створені в зашифрованому табличному просторі, автоматично шифруються. Шифрування табличного простору TDE доцільне, якщо таблиці містять конфіденційні дані в кількох стовпцях або якщо користувач хоче захистити всю таблицю, а не лише окремі стовпці. Користувачеві не потрібно виконувати детальний аналіз кожного стовпця таблиці, щоб визначити стовпці, які потребують шифрування. Крім того, шифрування табличного простору TDE використовує переваги масового шифрування та кешування для підвищення продуктивності. Фактичний вплив на продуктивність додатків може відрізнятися. Шифрування табличного простору TDE не шифрує дані, які зберігаються за межами табличного простору. Наприклад, дані BFILE не шифруються, оскільки вони зберігаються поза базою даних. Якщо користувач створює таблицю зі стовпцем BFILE у зашифрованому табличному просторі, цей конкретний стовпець не буде зашифрований. Усі дані в зашифрованому табличному просторі зберігаються на диску в зашифрованому форматі.

Шифрування табличного простору TDE також дозволяє сканувати діапазон індексів даних у зашифрованих табличних просторах. Це неможливо за допомогою шифрування стовпців TDE.

Oracle Database реалізує такі функції для шифрування табличного простору TDE:

- використання уніфікованого головного ключа шифрування TDE як для шифрування стовпців TDE, так і для шифрування табличного простору TDE;

- можливість користувачу скинути уніфікований головний ключ шифрування TDE, що забезпечує підвищену безпеку та допомагає відповідати вимогам безпеки та відповідності.

Отже, засоби TDE дозволяють негайно забезпечити шифрування даних без будь-якого кодування та складності управління ключами, що полегшує процес розробки захищених інформаційних систем.

Список використаних джерел:

1. Безопасность Oracle: шифрование данных пользователей. *Портал IT-специалистов: программирование, администрирование, базы данных.* URL: https://oracle-patches.com/oracle/secure/безопасность-oracle-шифрование-данных-пользователей (дата звернення: 16.05.2022).
2. Using Transparent Data Encryption with Other Oracle Features. *Moved*. URL: https://docs.oracle.com/database/121/ASOAG/using-transparent-data-encryption-with-other-oracle-features.htm#ASOAG10353 (date of access: 16.05.2022).

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

[1]***Погасій С. С.***

[1] *Національний технічний університет "Харківський політехнічний інститут" Навчально-науковий інститут комп'ютерних наук та інформаційних технологій м. Харків*

В доповіді проведено аналіз загроз щодо хмарних обчислень та розроблено їх класифікацію. Однією з проблем хмарних обчислень є труднощі, що виникають при переході на "хмару", найбільше це виявляється у двох напрямках:

Економічні витрати з його використання.

Інформаційна безпека, тобто. дані які зберігаються на хмарних сервісах, і при не дотриманні правил алгоритмів безпеки, схильні до ризику втрати інформації[1].

У цьому аспекті існує низка загроз:

Нездатність клієнта хмари самостійно контролювати та проводити аудит безпеки файлів, що обмежує його можливості.

Видалений злом або несанкціоноване проникнення в сервер хмар.

Низький рівень захисту бездіяльних віртуальних машин.

Використання практично виключно парольної автентифікації та застосування не цілком надійних способів відновлення забутих автентифікаційних даних [2].

Щоб мінімізувати всі ризики, потрібно чітко розуміти важливість усіх способів забезпечення конфіденційності та безпеки, особливо приділити увагу функціям шифрування та автентифікації даних усередині хмарного середовища, механізму контролю трафіку між машинами та розмежуванням прав на доступ.