17. *Сердюцкая Л.Ф.* Влияние некоторых параметров ТЭС на состав и количество загрязняющих веществ выбросах в атмосферу / Л.Ф. Сердюцкая, Н.А. Попова // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім Г.Є. Пухова НАН України. – Вип. 40. – К.: 2007. – С.73-82.
18. *Сердюцька Л.Ф.* До огляду моделей розповсюдження домішок в атмосфері міста / Л.Ф. Сердюцька, О.О. Попов // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім Г.Є. Пухова НАН України. – Вип. 45. – К.: 2008. – С.67-80.
19. *Швыряев А.А.* Оценка риска воздействия загрязнения атмосферы в исследуемом регионе: [учебное пособие для вузов] / А.А. Швыряев, В.В. Меншиков. – М.: Изд-во МГУ, 2004. – 124 с.
20. *Davies T.D.* Precipitation scavening of sulphur dioxide in an industrial area / T.D. Davies // Atmospheric Environment. – 1976. – №10. – P.879-890.
21. *McNaughton D.J.* Errors Inherent in Wind Inputs to Unliked Source and Dispersion Models / D.J. McNaughton // Air Waste Manage. Assoc. – 2010. – №7. – P.1018-1020.

Поступила 13.08.2018р.

УДК 519.7-004.65

М.Ю. Комаров, Київ
С.Ф. Гончар, Київ

АНАЛІЗ МЕХАНІЗМІВ БЕЗПЕКИ СИСТЕМИ УПРАВЛІННЯ БАЗАМИ ДАНИХ ORACLE DATABASE 12C ENTERPRISE EDITION

Abstract. Data base; The United Energy System of Ukraine, Real Application Cluster (RAC), Automatic Control Systems.

Актуальність

Надійна і стійка робота електроенергетики України значною мірою залежить від ефективної реалізації наявних можливостей і способів управління режимами роботи устаткування на усіх рівнях наявної ієрархічної системи управління.

Експлуатацію електроенергетичного устаткування здійснює оперативно-диспетчерський персонал, від рівня кваліфікації якого також залежить надійність енергопостачання споживачів.

Реалізація можливостей і способів управління режимами, у свою чергу, нерозривно пов'язана з процесами послідовного отримання оперативним персоналом центральних диспетчерських центрів (підприємств) достовірних вимірюваних або розрахункових даних про параметри режиму роботи електроенергетичних систем (ЕС) і завжди базується на різних інформаційних моделях елементів або окремих частин ЕС.

Сьогодні нестримно розвивається система глобальної світової

електроенергетики, утворена злиттям національних об'єднаних електроенергетичних систем (ОЕС).

Як приклад можна привести створення єдиного європейського електроенергетичного об'єднання (European Network of Transmission System Operators for Electricity) далі ENTSO=E (яке включає ЕС Франції, Іспанії, Португалії, Німеччини, Австрії, Італії, Бельгії, Голландії, Західної Данії, Швейцарії, Люксембурга, Словенії, Хорватії, Польщі, Чехії, Словаччини, Угорщини, Греції, Боснії і Герцеговини, Македонії, Сербії і Чорногорії, Албанії, Болгарії, Румунії, а також Великобританії і Ірландії, пов'язаних між собою і з континентальною частиною підводними кабельними лініями постійного струму), що являється по суті ОЕС Європи. У квітні 2011 р. Україна стала членом європейської Енергетичної Спільноти із затвердженням жорсткого графіку імплементації відповідних директив ЄС, в т.ч. і у сфері організації національного електроенергетичного сектора. Саме тому питання обліку, створення, накопичення, передавання та обробки великих інформаційних масивів про обладнання, режими функціонування та інші показники Енергосистеми України, на сьогоднішній день постають як ніколи актуально.

Сьогодні практично усі інженерні проекти за визначенням повного життєвого циклу енергетичного устаткування, що реалізовуються в передових країнах світу, базуються на застосуванні однакових інструментальних засобів - географічних інформаційних системах (ГІС), об'єднаних в ГІС-технології. Ці засоби застосовуються на усіх етапах проведення науково-дослідних робіт, проектування і виготовлення устаткування, подальшого монтажу і пуско-налагоджувальних робіт. Ці ж засоби також використовуються в процесі експлуатації устаткування і його подальшого демонтажу після закінчення запланованого терміну служби. Такий підхід дозволяє значно скоротити загальні витрати на впровадження нового устаткування і спростити процедуру його інтеграції в працюючі ЕС, полегшити процеси планування введення або виведення устаткування в планові ремонти, знижуючи таким чином експлуатаційну складову витрат на виробництво і передачу електроенергії споживачам.

ГІС-технологія базується на використанні сучасних системах управління базами даних (далі – СУБД), серед яких важливе місце займають ORACLE, PostgreSQL і MySQL. Перша і друга СУБД використовується для реалізації, як правило, масштабних проектів, а третя - для порівняно невеликих за об'ємом локальних проектів. В даній статті пропонується провести аналіз механізмів безпеки інформації, яка зберігається та обробляється в СУБД ORACLE. Аналіз буде проведено на прикладі СУБД ORACLE Database 12C Enterprise Edition.

Постановка задачі

Необхідно провести аналіз механізмів безпеки СУБД ORACLE Database 12C Enterprise Edition.

В дані статті пропонується розглянути механізми безпеки СУБД, які реалізовані підсистемою реєстрації подій, підсистемою резервування і відновлення, підсистемою забезпечення відмовостійкості та підсистемою контролю цілісності.

Вирішення задачі

Механізми безпеки інформації в СУБД ORACLE реалізовані засобами захисту від несанкціонованого доступу до інформації, які можуть використовуватися для реалізації функціональних послуг безпеки, описаних в НД ТЗІ 2.5-004-99.

Засоби захисту від несанкціонованого доступу до інформації реалізують ряд механізмів безпеки, що здійснюють в сукупності ідентифікацію та автентифікацію, розмежування доступу до об'єктів бази даних, реєстрацію подій і підтримку цілісності бази даних.

Підсистема реєстрації подій

Процедура аудиту являє собою процес реєстрації інформації про дії та події, що відбуваються в СУБД.

Можливо виділити 4 типи аудиту в СУБД:

1. Аудит інструкцій – реєстрація sql-інструкцій, виконуваних одним або більше (всіма) користувачами.

2. Аудит привілеїв – реєстрація застосування системних привілеїв одним (або більше) користувачем або всіма користувачами БД.

3. Аудит об'єктів схеми – реєстрація дій з одним або більше об'єктом в схемі.

4. Деталізований аудит – моніторинг доступу до даних на рівні їх вмісту (відносно інструкцій select, insert, update, delete).

Додатково можливо виділити аудит ресурсів – моніторинг ресурсів, виділених користувачеві.

Аудит виконується на рівні системних команд – наприклад, для створення об'єктів і управління ними.

Можливий аудит операцій з даними в БД або аудит задіяних системних ресурсів. Для реалізації аудиту дій користувачів з конкретною таблицею або набором таблиць - можливо задіяти механізм тригерів БД.

Зміни, що вносяться у важливі таблиці, також можливо реєструвати, створивши тригер, який буде перехоплювати значення до і після зміни, а також фіксувати додаткову інформацію.

СУБД пропонує виконання аудиту дій адміністраторів БД – активується зміною параметра AUDIT_SYS_OPERATIONS у файлі ініціалізації init.ora.

Ще одним об'єктом аудиту є процедура створення користувачів і об'єктів системи. Вбудовані засоби СУБД дозволяють автоматично перехоплювати різні дії з БД (запуск/зупинка екземпляра БД), команди DDL (Data Definition Language), які використовують для створення або модифікації структур БД (табличні області, файли даних).

Не проводиться реєстрація невдалого виконання збережених процедур - ні в ситуації, коли відбувається помилка авторизації, ні при зверненні до

неіснуючого об’єкту схеми. При некоректному написанні (синтаксисі), невдалий запуск процедури також не реєструється.

У разі, якщо допускається автоматичний запуск або зупинення БД (при запуску або зупинці ОС), записи будуть міститися також в журнал подій ОС.

Засоби аудиту СУБД дозволяють за допомогою однієї команди реалізувати аудит додавання нових таблиць до БД або здійснювати реєстрацію застосування привілеїв конкретним користувачем.

Для включення аудиту необхідно присвоїти одне із зумовлених значень (TRUE, FALSE, NONE, DB, DB_EXTENDED або OS) параметру AUDIT_TRAIL у файлі ініціалізації init.ora. Дані аудиту зберігаються в журнал ОС або таблицю БД - AUD$ схеми SYS. Для активації функції аудиту потрібна наявність у користувача привілеї Audit System, Audit Any.

Залежно від типу активованого аудиту, можливо зберігати в журналі аудиту різні дані, але завжди реєструються:

- ідентифікатор або ім’я користувача;
- ідентифікатор сеансу;
- ідентифікатор термінала;
- ім’я схеми об’єкта, до якого відбувається звернення;
- виконувана операція (або спроба її виконання);
- код завершення операції;
- дата і час;
- використовувані системні привілеї.

Для зручності сприйняття інформації, що зберігається в таблиці SYS.AUD$, в СУБД реалізовано низку уявлень, які поділяються на підгрупи DBA_, ALL_ і USER_. Кожне з них повертає підмножину інформації з таблиці SYS.AUD$.

Щоб сформувати необхідний набір таблиць і уявлень аудиту, потрібно виконати скрипт cataudit.sql, що входить до складу СУБД.

СУБД не передбачає засобів автоматичного видалення даних з таблиці AUD$, але дозволяє видаляти інформацію вручну з цієї таблиці або виробляти її усічення (truncate).

Тригери являють собою збережені процедури, які виконуються у відповідь на операції і події, пов’язані з ними що відбуваються в базі даних:

- перевірка внесених до таблиці змін;
- автоматизація супроводу бази даних;
- установка обмежень на виконання операцій над об’єктами бази даних.

Передбачено наступний перелік подій і структурних компонентів процесу обробки даних, з якими можна пов’язувати тригери:

- інструкції мови маніпулювання даними (DML). Тригери DML запускаються у відповідь на вставку, оновлення або видалення рядка таблиці бази даних;
- інструкції мови визначення даних (DDL). Інструкція DDL – будь-яка SQL-інструкція, що створює або модифікує об’єкт бази даних, такий

як таблиця або індекс. Тригери DDL запускаються у відповідь на виконання DDL-інструкцій. З їх допомогою можливо виконувати аудит і забороняти певні операції;

- події бази даних. Тригери подій використовуються при її запуску і зупинці, при підключенні і відключенні сервера, у випадку виникнення помилок. Дозволяють контролювати активність БД;
- тригери INSTEAD OF (тригери, що заміщають). Тригери, що заміщають запускаються перед операціями DML – їх код визначає, які дії слід виконати замість відповідної операції. Вони управляють операціями над поданнями, але не над таблицями;
- призупинені інструкції. Якщо в ході виконання інструкції виникла проблема доступності простору, СУБД може перевести її в режим призупинення до тих пір, поки ця проблема не буде вирішена;

Всі тригери поділяються на:

- тригер BEFORE. Викликається до внесення будь-яких змін, у тому числі до вставки запису (BEFORE INSERT);
- тригер AFTER. Виконується після того, як проводяться всі зміни;
- тригер рівня інструкції. Виконується для окремої SQL-інструкції, яка обробляє одну або більше записів бази даних;
- тригер рівня запису. Викликається для окремого запису,який оброблюється SQL-інструкцією.

Аудит привілеїв являє собою вибірковий (виборчий) аудит операторів, дозволений користувачам, що володіє системними привілеями. Можливо дозволити аудит використання будь якої системної привілеї.

При використанні аудиту привілеїв, власники цих привілеїв, так само як і привілеї об’єктів схеми контролюються в першу чергу, а потім вже здійснюється контроль системних привілеїв.

Аудит привілеїв є більше спеціалізованим порівняно з аудитом операторів через те, що кожна опція аудиту виконує аудит лише певних типів операторів, не обов’язково пов’язаних чим-небудь між собою. Подібно до аудиту операторів, аудит привілеїв дозволяє робити аудит діяльності усіх або окремих користувачів БД.

Аудит об’єктів схеми є виборчим аудитом окремих DML (Data Manipulation Language) – операторів, а також операторів GRANT і REVOKE для певних об’єктів схеми. Аудит об’єктів схеми робить аудит операцій, допущених привілеями об’єктів схеми – таких як оператори SELECT або DELETE по відношенню до певної таблиці, так само як і оператори GRANT і REVOKE, контролюючі ці привілеї.

Є можливість робити аудит операторів, що відносяться до таблиць, подання, послідовностей, процедурам, що зберігаються та функціям і пакетам.

Механізм FGA (Fine – Grained Auditing – деталізований аудит) це гнучкий інтерфейс для аудиту операторів SELECT, INSERT, UPDATE, DELETE у рамках таблиць і подання на підставі їх вмісту.

З використанням пакету DBMS _ FGA, можливо створити політику аудиту відносно конкретної таблиці. Якщо який-небудь рядок таблиці, який повертається по блоку запитів, задовольняє умові аудиту, у такому разі запис аудиту, що містить ім'я користувача, текст SQL, пов'язану змінну, назву політики, ID сеансу, тимчасову мітку і інші атрибути, буде занесена в журнал аудиту.

Додатково можливо визначати обробник події аудиту, для внесення запису – наприклад, обробник події аудиту може послати повідомлення про порушення політики безпеки адміністратору.

Для реалізації аудиту операторів, привілеїв і об'єктів схеми, СУБД пропонує можливість здійснення виборчого аудиту вдалого і невдалого виконання операторів, або ж обох відразу.

Використовуючи будь-яку форму оператора AUDIT, можливо включити в нього:

- вираз WHENEVER SUCCESSFUL, для аудиту тільки успішно виконаних операторів;
- вираз WHENEVER NOT SUCCESSFUL, для аудиту невдало (несанкціонованого) виконаних операторів.

Вирази BY SESSION, BY ACCESS, BY USER аудиту операторів:

- BY SESSION – для будь-якого виду аудиту (об'єкту схеми, оператора, або привілею), робиться вставку одного запису в журнал аудиту, для кожного користувача і об'єкту схеми, впродовж сеансу роботи - проміжку часу між моментом, коли користувач з'єднується з БД і відключається від неї;
- BY ACCESS – виконується вставка одного запису аудиту в журнал при кожному виконанні операції, що піддається реєстрації;
- BY USER – аудит операторів, ініційованих будь-яким користувачем або операторів, ініційованих певним списком користувачів.

Підсистема резервування і відновлення

У СУБД існують наступні механізми резервування і відновлення.

Фізичне резервування (physical backup) полягає в резервуванні файлів (файлів даних, керуючих файлів, архівних журналів повторного виконання). СУБД дозволяє виконувати резервування як з необхідністю зупинки системи, так і при працюючій системі. Резервні файли використовуються для архівного зберігання і відновлення бази даних. Причому, резервні файли даних і керуючі файли, використовуються для відновлення бази даних за станом на момент виконання повного резервування, а архівні файли журналу повторного виконання використовуються для відновлення системи до довільного моменту, що знаходиться після моменту виконання процедури повного резервування, і дозволяють відновити усі підтверджені транзакції, що сталися у БД.

Логічне резервування (logical backup) полягає в резервуванні об'єктів СУБД (таблиць, процедур, що зберігаються, і так далі). Цей тип резервування виконується за допомогою утиліти СУБД Export і може резервувати не усю

базу даних, а окремі її елементи. З метою подальшого відновлення об'єктів використовується утиліта СУБД Import.

Підсистема забезпечення відмовостійкості

СУБД надає декілька способів забезпечення відмовостійкості, відмінних за мірою захисту, вартості і величині необхідних ресурсів апаратного забезпечення. Вони можуть бути використані як окремо так і одночасно.

Real Application Cluster (RAC)

Технологія Oracle Real Application Clusters (RAC) дозволяє будувати відмовостійкі і масштабовані інформаційні системи, об'єднуючи сервери в кластери.

Oracle RAC дозволяє декільком екземплярам СУБД, що функціонують на різних апаратних вузлах, працювати з єдиною базою даних. При цьому не вимагається вносити модифікації в клієнтське програмне забезпечення, для якого кластеризована база даних доступна як єдиний логічний екземпляр, як і для інсталяцій без RAC.

Кожен додатковий вузол кластера забезпечує додаткові обчислювальні ресурси для обробки даних, у тому числі підтримані паралелізування запитів між вузлами кластера, конвеєрний паралелізм, і тим самим забезпечується масштабованість сервера бази даних. У разі збою одного з вузлів кластера, програмне забезпечення RAC переносить усі сесії на інший вузол. Також RAC забезпечує програмне балансування навантаження між вузлами

Oracle Fail Safe (Cold Failover Cluster)

Суть цієї технології полягає в тому, що дискове сховище з базою даних розділяється між двома фізичними серверами. Але одночасно з дисковим сховищем (тобто з базою даних) працює тільки один з екземплярів СУБД, а другий екземпляр знаходиться в постійному очікуванні і не підтримує в цьому режимі клієнтських підключень.

У разі виходу з ладу робочого сервера в справу вступає резервний, який продовжує роботу з того ж моменту, з якого припинив роботу основний.

Переключення користувачів на резервний сервер і активізація резервного сервера відбуваються в повністю автоматичному режимі. Для користувачів це відбувається абсолютно прозоро, вони не дізнаються про те, що стався вихід з ладу робочого сервера і перемикання на резервний.

Standby Data Guard

Технологія Oracle Data Guard пропонує рішення для забезпечення високої доступності, підвищеної продуктивності і автоматичного подолання наслідків збою.

Зміни в основній базі даних можуть бути передані в резервні бази даних з гарантією відсутності втрат даних в процесі передачі.

Підтримуються 2 типи резервних баз даних – із здійсненням фізичного і логічного резервування.

Фізична резервна база даних містить ті ж самі структури, що і основна. Логічна – може мати інші внутрішні структури (наприклад, додаткові індекси, використовувані для генерації звітів). Синхронізація основної бази даних з

резервними здійснюється шляхом передачі журнальних даних через SQL – оператори, що виконуються над резервною базою даних.

Фізична резервна база даних є поблочною копією первинної бази даних. Під час відновлення в аварійних ситуаціях, резервна база даних в точності схожа на основну базу даних.

Логічна база даних – використовується для підготовки звітів (при підготовці звітів потрібно істотні ресурси системи). В цьому випадку резервна база даних відкривається тільки для читання і користувачі, яким необхідно сформувати звіти працюють з нею. При цьому основна база даних продовжує працювати на прийом даних від користувачів.

Підсистема контролю цілісності

Контроль цілісності виконавчих файлів

Установка програмного забезпечення СУБД здійснюється за допомогою утиліти Universal Oracle Installer, що представляє собою Java-програму і має графічний інтерфейс користувача. Однією з основних функцій утиліти є формування файлів репозиторія Oracle Inventory, в якому крім інформації про встановлені програмні компоненти і модулі містяться дані про контрольні суми MD5 виконавчих двійкових файлів вихідного дистрибутива.

При запуску екземпляра СУБД здійснюється зрівняння контрольної суми MD5 програмного файлу, що запускається зі значенням, зазначеним у Oracle Inventory. Факт розбіжності контрольних сум зазначається окремим записом у журнальному файлі системних подій ALERT.LOG. Моніторинг та аналіз подій у файлі ALERT.LOG може здійснюватися в автоматичному режимі засобами Oracle Enterprise Manager.

Контроль цілісності інформації в БД

СУБД забезпечує:

- цілісність даних;
- посилальну цілісність;
- цілісність транзакцій.

Цілісність даних визначається правилами перевірки достовірності даних, які гарантують, що недійсні дані не потраплять у таблиці. СУБД дозволяє визначати і зберігати ці правила для об’єктів БД, яких вони стосуються, таким чином, щоб кодувати їх тільки одного разу. При цьому вони активуються всякий раз, коли який-небудь вид зміни проводиться в таблиці, незалежно від того, який процес виконує вставки, модифікації або видалення. Цей контроль здійснюється у формі обмежень і тригерів БД. Обмеження – це правила, застосовні до таблиць під час або після створення, поширювані на те, як ці таблиці можуть заповнюватися.

Посилальна цілісність – це обмеження бази даних, що гарантує, що посилання між даними є дійсно правомірними і неушкодженими.

Цілісність транзакцій – дотримання вимог ACID (Атомарність, Узгодженість, Ізоляція, Довговічність) в процесі передачі транзакційних даних між вихідною і цільовою системами. Це забезпечує цілісність у рамках всієї топології реплікації (промислові, резервні, звітні бази даних).

Встановлення з'єднання клієнт-сервер

Для конфігурування та управління мережевими підключеннями СУБД має набір служб Oracle Net Services, що представляє собою комплект компонентів, які надають рішення для забезпечення можливості підключення в розподілених комп'ютерних середовищах. Набір Oracle Net Services складається з служб Oracle Net (Мережа Oracle), Oracle Net Listener (Служба прослуховування мережі Oracle), Oracle Connection Manager (Диспетчер підключень Oracle), Oracle Net Configuration Assistant (Помічник по конфігурації мережі Oracle) і Oracle Net Manager (Диспетчер мережі Oracle). Програмне забезпечення Oracle Net Services встановлюється автоматично в процесі інсталяції програмного забезпечення Oracle Database Server (Сервер баз даних Oracle) або Oracle Client (Клієнт Oracle).

Oracle Net – програмний компонент, який ініціює, встановлює і підтримує підключення між клієнтами і серверами. Тому компонент Oracle Net повинен бути встановлений як на клієнті, так і на сервері. Oracle Net складається з наступних двох основних компонентів:

- Oracle Network Foundation Layer (Базовий мережевий рівень Oracle). Відповідає за встановлення та підтримку з'єднання між клієнтським додатком і сервером, а також за обмін повідомленнями між ними.
- Oracle Protocol Support (Підтримка протоколу Oracle). Відповідає за відображення функціональності TNS (Transparent Network Substrate – Прозоре мережеве середовище) на стандартні протоколи, використовувані при підключеннях.

Всі сервери, що містять базу даних Oracle, виконують також службу Oracle Net Listener, служба прослуховування мережі Oracle (зазвичай званий просто слухачем), основна функція якої – прослуховування запитів клієнтів на вхід в базу даних Oracle. Переконавшись, що служба клієнта володіє відповідною інформацією бази даних (протоколом, портом і ім'ям примірники), слухач передає запит клієнта базі даних. База даних дозволить клієнтові виконати вхід, якщо, звичайно, справжність його імені користувача і пароля підтверджуються. Як тільки слухач передає запит користувача базі даних, клієнт і БД опиняються в безпосередньому контакті, що не вимагає ніякої допомоги з боку служби прослуховування.

Усі налаштування механізмів захисту СУБД зберігає в таблицях словника даних, і адміністратор може здійснювати контроль цих налаштувань за допомогою спеціалізованих DBA _, ALL _ або USER _ подань.

Висновки

Проведено аналіз механізмів захисту інформації системи управління базами даних Oracle Database 12C Enterprise Edition. В рамках проведення аналізу розглянуті такі підсистеми, як підсистема реєстрації подій, підсистема резервування і відновлення, підсистема забезпечення відмовостійкості, підсистема контролю цілісності, а також механізм встановлення з'єднання клієнт-сервер.

За результатами проведеного аналізу встановлено, що СУБД реалізує систему розпізнавання, фіксування і аналіз подій, що пов'язані з підтриманням політики безпеки інформації з метою контролю небезпечних для СУБД дій.

Отримані результати дозволяють констатувати можливість застосування СУБД Oracle Database 12C Enterprise Edition як основу для побудови ГІС-систем на етапах проведення науково-дослідних робіт, проектування і виготовлення устаткування енергетичних систем, його подальшого монтажу і пуско-налагоджувальних робіт.

1. *В.А. Гуреев, В.Н. Сулейманов, О.В. Сулейманова, Н. Реза*. Принципы построения информационной части модели электроэнергетики Украины. // Электропанорама, № 12, 2011.
2. *Гуреев В.А., Сулейманова О.В*. Разработка архитектуры мини базы знаний противоаварийных тренировок // Энергетика и электрификация. 1987. – № 1, С.44-46.
3. *Гуреев В.А., Редковский Н.Н., Суманенков В.Г*. Информационная технология управления сложными распределенными техническими системами. // Информационные технологии и новейшее применение теории управления (Автоматика-94): Тез. докл. 1-й Украинской конф. по авт. упр. – К.: 1994. – Ч. 1, С.230-231.
4. *Рик Гринвальд, Роберт Стаковьяк, Джонатан Стерн.* Oracle11g. Основы – Символ-Плюс, 2009. – 464 с.
5. *С. Фейерштейн, Б. Прибыл.* Oracle PL/SQL. Для профессионалов – Питер, 2011. – 800 с.
6. Oracle® SQL Developer User's Guide.

Поступила 10.09.2018р.

УДК 004.056:004.75

М.Р. Шабан, Київ

АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ ПЕРЕВІРКИ ПОВНОТИ ТА НЕСУПЕРЕЧНОСТІ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИСТУ

Abstract. In this article, the algorithm of the Module "identification of the functional protection profile" was considered. This algorithm was divided into two subtasks. At the first stage, the compliance of the functional protection profile with the formal criteria was determined. At the second stage, criteria were determined for compliance with functional security services in the process of semantic analysis in the input documents.

У попередній роботі [2] мною була розглянута процедура формалізації правил перевірки повноти та несуперечності функціонального профілю

